24 口全千兆远程管理型交换机

7324NSW

深圳市磊科实业有限公司

Shenzhen Netcore Industrial Ltd.

Http://www.netcoretec.com

目　录

第一章 前 言

1.1 公司简介

衷心感谢您选用 NETCORE 产品！您将得到长期、全面和高质量的服务！

NETCORE 公司 1988 年正式成立于台湾，是新竹工业园早期创业者之一，作为国际知名的网络通信专业厂商，主要从事于局域网络、无线网络、SOHO 网络以及通讯产品研发、生产和销售。公司本着“诚信”的经营理念，依靠强大的技术背景，在 90 年代迅速崛起。目前拥有强大的研发和生产能力，分支机构遍及全球，在客户中博得广泛赞誉。

NETCORE 中国公司于 2000 年 10 月正式宣布成立，现已在中国地区设立了一个营销中心，一个生产基地和两个研发中心，并在国内主要中心城市建立了 10 多个销售办事处，辐射全国网络市场。

NETCORE 中国公司旨在为国内用户提供经济、高效、实用的全面网络解决方案，产品包括网卡、集线器、交换机、路由器、调制解调器等多个系列。并致力于三层到七层交换、全光网等前端科技的研发与应用。2000 年 11 月，NETCORE 成为首家在国内市场上推出千兆铜缆交换机的网络厂商。

“专业、优质、创新”，NETCORE 中国公司将与广大用户一起迎接信息时代的挑战！

1.2 用途

本手册的用途是帮助你便捷和正确地使用 Netcore 7324NSW 二层交换机。在您准备使用本产品之前，请仔细阅读本手册，以方便、快捷的使用本产品的所有功能。

1.3 约定

在阅读本手册时，敬请注意下列事项：

**温馨提示**：在使用交换机需要注意的一些事项

**重要提示**：在使用交换机需要特别注意的事项

**友情提示**：在使用交换机过程中必要的解释信息

1.4 版权、商标声明

第二章 认识 Netcore 7324NSW 交换机

2.1 产品特性

Netcore7324NSW 交换机是磊科公司新近推出的一款高性能、多用途、高安全性的二四层网管型交换机。

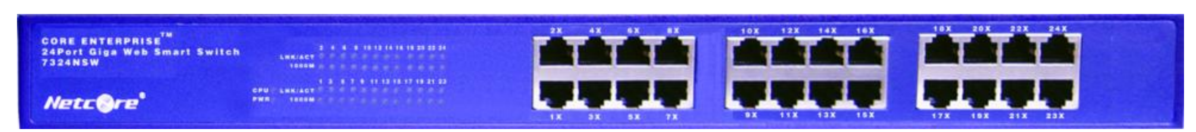


图 2.1 Netcore 7324NSW 外观示意图片

2.1.1 硬件特性

- 7324NSW支持48G背板带宽
- 10/100/1000Mbps自适应以太网端口，完全自动侦测并适应10/100/1000Mbps以及半双工、全双工链路，也可以根据用户的需要进行强制速率、双工设置
- 以太网端口自动侦测双绞线缆的类型（AUTO-MDIX），并自动适应不同类型的线缆
- IEEE 802.3x流量控制保证了数据帧可靠传输，使数据帧的传输损失率极大地降低
- 支持静态链路聚合，可以自动将多条物理链路合并成一条高速逻辑链路，同时起到了容错作用

2.1.2 网络协议

- 虚拟局域网（VLAN）：支持基于802.1QVLAN（Tagged VLAN），遵从IEEE 802.1q文档规范

2.1.3 网络应用

- 支持MAC地址绑定
- 支持MAC地址过滤
- 支持MAC地址学习管理
- 支持MAC地址老化管理
- 支持基于端口的捕获

2.1.4 支持强大 QoS 能力

Netcore 交换机提供多种流分类技术和多种 QoS 技术，包括 802.1p、WRR、DSCP，为各种应用的带宽保障提供需要的支持技术。

- 流分类：支持802.1P、端口优先级。
- 流标记：802.1p是二层协议，可以为数据提供8个级别的优先级标记。
- 队列调度：Netcore 7324NSW 二四层层网管交换机支持严格优先级队列与加权循环队列两种对列调度方式。
- DSCP：使用三层的协议头，做为QOS依据。

2.1.5 管理方式

- 支持基于WEB的管理
- 支持串口方式下的管理配置（仅限于恢复默认参数和升级）

2.1.6 系统升级、参数备份和恢复

- 支持基于WEB方式的固件升级
- 支持基于X-Modem的固件升级
- 用户在交换上所作的配置参数可以备份到本地存储器上，然后根据需要随时恢复任何一个备份的配置参数

2.2 面板布置

2.2.1 前面板

Netcore 7324NSW 二层交换机的前面板上有 24 个 10/100/1000Mbps 铜缆/组合端口。

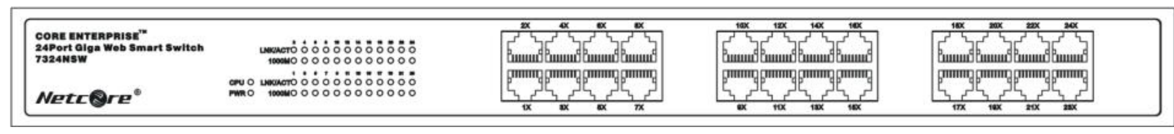


图 2.2 Netcore 7324NSW 前面板示意图片

- 10/100/1000Mbps自适应的UTP端口，以便与PC、服务器、其它HUB或交换机、路由器相连。支持自动线序交换的功能，与其它设备可采用交叉线或直连线进行连接。
- 交换机提供10/100/1000Mbps铜组合千兆端口
- 提供易于理解的LED状态指示灯，便于诊断网络上所发生的各种问题和故障。详见“2.2.4 LED指示灯”一节。

2.2.2 后面板

Netcore7324NSW 二层交换机的后面板上有 1 个电源接口，1 个 Console 控制口



图 2.3　Netcore 7324NSW 交换机后面板示意图片

- 后面板上的交流电源接口是标准的三相接口，支持220V AC 50Hz
- 1个Console（RS-232）控制口，以便通过对其交换机进行管理

2.2.3 侧面板

Netcore 7324NSW 二层交换机的侧面板上有很多个通风孔，用于散热用途。

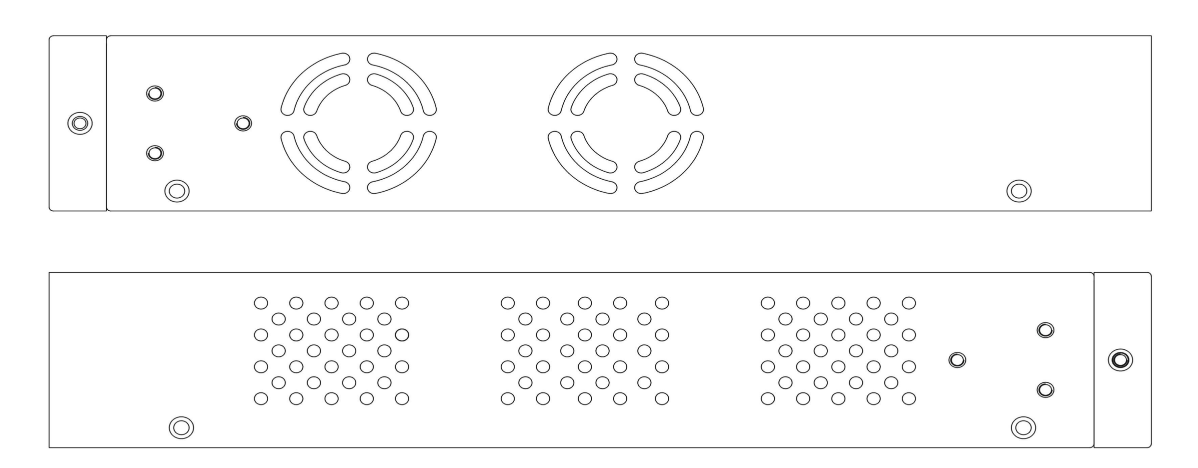


图 2.4　Netcore 7324NSW 侧面板示意图片

交换机侧面有散热风扇，用于进行有效的降温散热，以保证交换机的正常工作。交换机工作时请勿覆盖该通风孔。

2.2.4 LED 指示灯

通过 Netcore 7324NSW 二四层交换机前面板上的 LED 指示灯，可以方便、实时地观察交换机上的各种工作状态，便于诊断所发生的问题和故障。

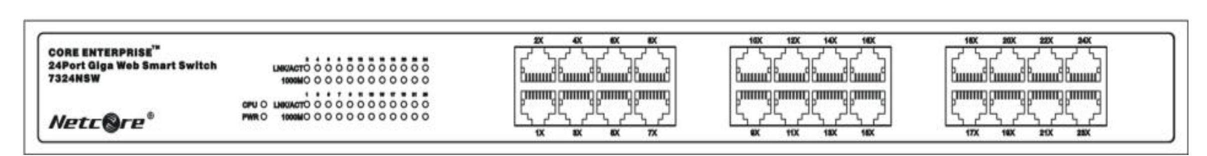


图 2.5 Netcore 7324NSW LED 指示灯示意图片

指示灯	颜色	描　述
PWR	绿色	常亮：加电正常
CPU	绿色	常亮：交换机里面的程序启动后，此指示灯长亮
1000M	绿色	常亮：模块端口与所连接的设备以 1000Mbps 速率工作 闪亮：有数据正在发送或者接收时
		不亮：无
LINK/ACT	绿色	常亮：模块端口与所连接的设备以 1000Mbps 速率工作 闪亮：有数据正在发送或者接收时
		不亮：无

2.2.5 技术指标

- 端口符合标准

IEEE802.3 10BASE-T/802.3u 100BASE-TX，IEEE 802.3ab 1000Base-T 千兆以太网标准
ANSI/IEEE 802.3x NWay自动协商
10/100/1000M速度全/半双工
全双工IEEE 802.3x 流量控制

- 网络介质：

10Base-T－UTP/STP 3 类或 5 类双绞线
100Base-TX - UTP/STP 5 类双绞线
1000Base-T-UTP/STP 5 或 5E 类双绞线

- 端口类型

24 个屏蔽 RJ45 接口
1000BASE-T 端口

- 性能

传输方式: 存储转发
MAC 地址表: 每个设备 16K 条目
MAC 地址学习
动态条目:自动更新
静态条目:用户定义

- 二层包转发速率（半双工）

以太网：每端口最大线速转发 10Mbps
快速以太网：每端口最大线速转发 100Mbps
千兆以太网：每端口最大线速转发 1000Mbps

- 硬件参数指标

	7324NSW
工作温度	0℃ 到 50℃
存储温度	-20℃ 到 70℃
工作湿度	10% 到 90% RH
存储湿度	5%到 90%RH

输入电源	AC 100-240V 50-60Hz
功耗	约 21W
机械尺寸	432mm×250mm×44mm
重量	3.0KG
认证	FCC PART15 CE
噪音	25分贝

第三章 安装方法

3.1 安置方法

首先请按照下述步骤妥当地安置好交换机:

- 必须放在至少能承重4kg的表面上
- 供电的电源插座距离交换机须在1.82米之内
- 确保电源线已可靠地连接在交换机后面板上的电源接口和供电的电源插座之间
- 保证交换机的四周可以良好的通风散热并且请勿将重物放置在交换机上

3.2 安装在桌面上的方法

当欲将交换机安装在桌面上时，需先将包装箱内提供的 4 个黏性胶垫粘贴在交换机底面的四角的相应位置，然后，再将交换机平放在桌面上,以确保交换机的周围的空气能够良好地流动通风。

3.3 安装在机架中的方法

交换机可以被安装在标准的 19 英寸的机架内。首先，需要将包装箱内已提供的上机架的配件用与其配套的螺丝固定在交换机的前面板的两侧，然后，再用螺丝将交换机安装在 19 英寸的机架内。

3.4 加电

交换机的输入电压范围是 100-240 VAC（50-60Hz）的交流电，交换机的内置电源系统可以根据实际输入的电压自动调整其工作电压。电源接口位于交换机的后面板上，请将电源线一头插在交换机后面板上的电源接口上，另一头插在电源插座上。

交换机通电后交换机上的 LED 指示灯将会出现如下反应：

- “PWR”指示灯长亮，所有LED指示灯将快速闪亮一下。
- “CPU”指示灯将持续长亮，表示交换机已处于工作状态。
- 端口状态指示灯将亮或者灭，依赖于对应模块端口的连接状态。


重要提示

当供电系统出现掉电故障时，为了确保交换机不被突发性的大电流而损坏，请务必将交换机的电源线从供电的插座上拔下来。当供电恢复正常后，再将交换机的电源线插上。

第四章 交换机的连接方法

4.1 交换机的连接

交换机前面板提供 24 个 1000BASE-T RJ-45 端口，这 24 个端口能自动侦测网络速度、自动适应双工状态。

本交换机能够连接工作站 PC、服务器、集线器、路由器、网桥、中继器或其他交换机。

4.2 与网络最终节点的连接方法

连接网络终节点请用 3 类或 3 类以上的非屏蔽或屏蔽双绞线连接交换机 RJ-45 接口和网络终节点 RJ-45 接口。本交换机具有 AUTO-MDI/MDIX 自动线序交叉功能，直连线和交叉线都能连接本交换机。

在 10Base-T 以太网必须使用 3 类或 3 类以上的屏蔽或非屏蔽双绞线。

在 100Base-TX 快速以太网必须使用 5 类或 5 类以上的屏蔽或非屏蔽双绞线。

在 1000Base-T 千兆以太网必须使用 5e 类屏蔽或非屏蔽双绞线。

通过双绞线连接交换机与网络最终节点时双绞线的长度请不要超过 100 米。

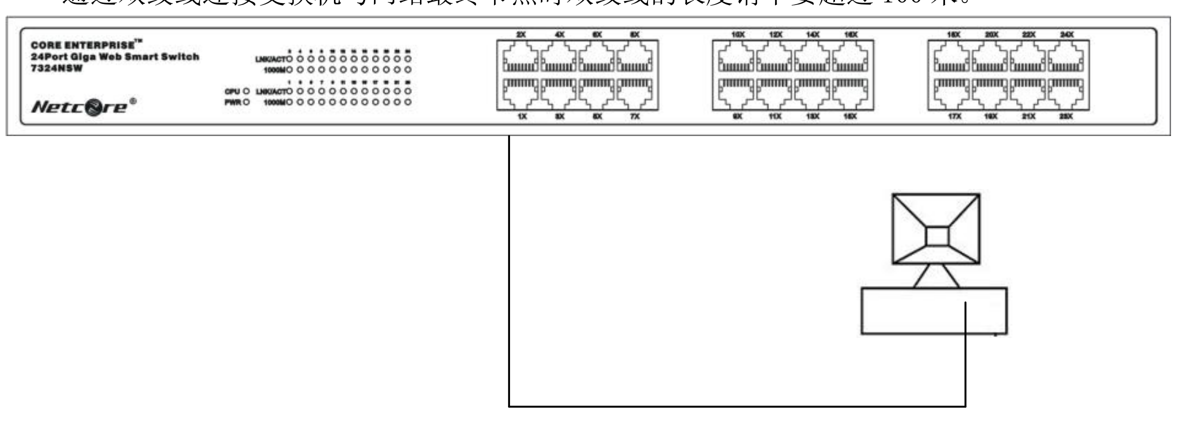


图 4.1


温馨提示

如果连接正确对应端口的 LED 指示灯将出现如下反应：

1：当所连接的设备正常连接到交换机，并且所连接的设备开机时，“ACT”指示灯将长亮

2：如果相应的 LED 指示灯不亮，请检查网卡的安装、网线的连接等是否正确。

4.3 与其它 HUB 或交换机的连接方法

将 Netcore 7324NSW 二四层交换机与其他网络设备采用直联线或交叉线直接相连。

1:10BASE-T 的 HUB 或交换机与 7324NSW 相连时,可以使用 3 类、4 类或者 5 类或以上的 UTP/STP 双绞线。

2：100BASE-T 的 HUB 或交换机与 7324NSW 相连时，必须使用 5 类或以上的 UTP/STP 双绞线。

3：1000BASE-T的网卡或交换机与7324NSW相连时，必须使用超5e类或以上的UTP/STP双绞线。

第五章 配置您的交换机

5.1 概述

Netcore 7324NSW二四层交换机可采用一种方式进行管理：

- 基于Web界面的管理（HTTP）
- 控制台（CONSOLE）方式管理（ 注：此CONSOLE管理只用于X-MODEM升级跟恢复默认参数。配置任何参数时，还需到WEB页面上配置。）

基于Web页面的管理方式简单易学，用户利用Microsoft Internet Explorer浏览器可以迅速对Netcore 7324NSW二四层交换机进行管理配置。

下面分别介绍使用基于Web页面（HTTP）和控制台（CONSOLE）方式进行管理的简要用法。

以下的操作均在Microsoft Windows系列操作系统中进行。

5.2 管理方式

5.2.1 Web 管理方式（HTTP）

这种管理方法类似于访问一个网站，由于采用TCP/IP协议，可以实现远程管理。

首先按照下面示意图建立好TCP/IP网络连接：

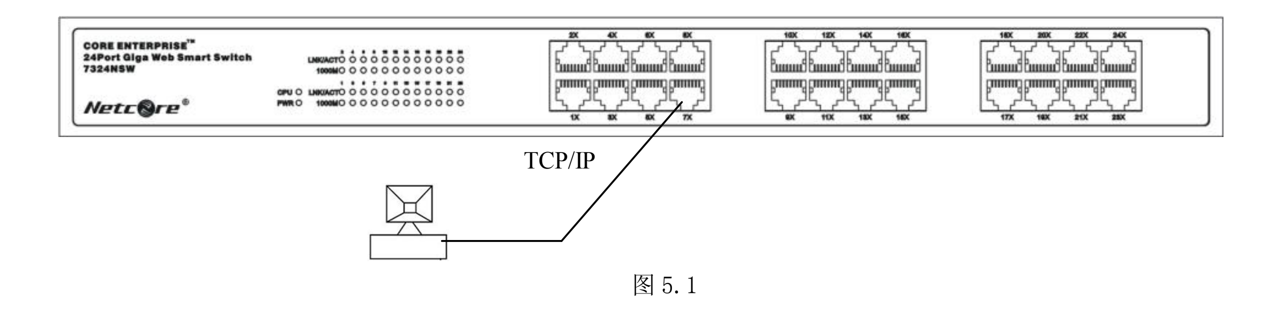


图 5.1

打开Windows系统中的Internet Explorer程序（推荐使用IE5.0以上），在地址栏里输入交换机的IP地址。



Netcore 7324NSW二四层交换机的WEB登录页面，如图所示：



图 5.2

用户可以输入用户名和密码，进入交换机的WEB管理页面。



温馨提示

出厂时交换机的默认用户名为 admin，密码为 netcore。

Netcore 7324NSW二四层交换机的管理主页如图5.3所示：



图 5.3　7324NSW 主页

5.2.2　控制台方式（CONSOLE）

控制台方式是通过Microsoft Windows的超级终端对交换机进行管理和配置。这种方式可以方便地通过PC的串行口对设备进行管理，由于该方式不依赖于网络连接，所以当出现链路故障时，通常使用这种方式进行检测。

该连接方法请参考前面有关章节。

注：此CONSOLE管理只用于X-MODEM升级跟恢复默认参数。配置任何参数时，还需到WEB页面上配置。

- 恢复默认：将串口（CONSOLE）线插好后，通电，一直按住键盘上“D”不放，大概15秒后，在任务栏的通知区域内，但到连接断开，再连接好后，表示恢复默认成功。

```
FLASH area check:
  Checking Application 1 Area... 7324NSW

if you want to update program with XMODEM,press X...

Loading 7324NSW program...
Begin uncompress program....
this will take some time,please wait...
uncompress OK!

    ***************************************************************
    * Welcome to use Netcore Products                             *
    * Copyright 2004 by Netcore Inc. All rights reserved.         *
    * Netcore network products series                             *
    ***************************************************************

Waiting 2 seconds : Press <d> for default parameteres
Load Parameters Failed! Loading default parameters.
```

图 5.4

- X-MODEM升级：恢复默认：将串口（CONSOLE）线插好后，通电，一直按住键盘上“X”不放，等出现有“C”显示出现，在菜单栏中找到传送，然后将要升级的文件传送上去就好。一定要在传送文件协议处选择Xmodem升级。

```
FLASH area check:
  Checking Application 1 Area... 7324NSW

if you want to update program with XMODEM,press X...

Prepare the file in XModem client.
CCCCCCCCCCCCCCC_
```

图 5.5


发送文件
文件夹: C:\Documents and Settings\jyt
文件名(F):
浏览(B)...
协议(P):
Xmodem
发送(S)
关闭(C)
取消

图 5.6

第六章 交换机的功能配置指南

在前面章节5.2.1我们已经详细介绍了如何使用交换机的WEB配置管理，下面以WEB配置为例具体介绍交换机各种功能的使用。介绍顺序以交换机主菜单栏为索引。

6.1 系统管理

6.1.1 IP 地址

设置Netcore 7324NSW二四层交换机的IP地址。（默认IP地址为192.168.2.11），用户可以任意设定所需要的IP地址。

具体操作：在“IP地址”的配置页面上输入新的IP地址和子网掩码和网关地址。点击确定完成IP地址设置。配置网关地址可以使主机跨网段登陆交换机进行配置。如图所示：

IP地址配置	
IP地址：	192.168.2.11
子网掩码：	255.255.255.0
网关：	192.168.2.1
	确定

图 6.1

6.1.2 修改密码

设置管理Netcore7324NSW二四层交换机的管理密码（默认为netcore）。

具体操作：在帐户管理的设定页面上输入旧密码、新密码和确认密码。如图所示：

修改密码

旧密码	
新密码	
确认密码	

确定

图 6.2

6.1.3 MAC 地址

设置Netcore 7324NSW二四层交换机的MAC地址。

具体操作：在“MAC地址”配置页面上输入新的MAC地址。如图所示：



图 6.3

6.1.4 CONSOLE 信息

查看登录Netcore 7324NSW二四层交换机CONSOLE口管理配置信息。如图所示：

Console 信 息

数据位:	8
停止位:	1
奇偶校验:	none
传输流控:	none
波特率(bps):	9600

图 6.4

6.1.5 管理 VLAN

通过管理 VLAN 限制只能设置属于此 VLAN 的端口才能登录交换机进行配置。不启用则所有 VLAN 下面的端口都能同时登陆交换机进行配置。

例如：限制属于 VID 为 1 主机才能登陆交换机进行配制。



图 6.5

6.1.6 系统升级

通过WEB可以对Netcore 7324NSW二四层交换机软件进行本地升级。点击“浏览”选中保存在本地的升级文件，然后“开始升级”当“系统升级状态”中提示升级成功后，表示用户系统升级成功。



图 6.6

重要提示

在升级过程中，不能拔掉电源，否则会导致升级失败。

6.1.7 参数保存

所有的参数配置好后，对Netcore 7324NSW二四层交换机的配置参数进行保存，如果不作参数保存的话，当前配置的参数仅在此次配置上生效，下次重新启动后，配置的参数将会丢弃。

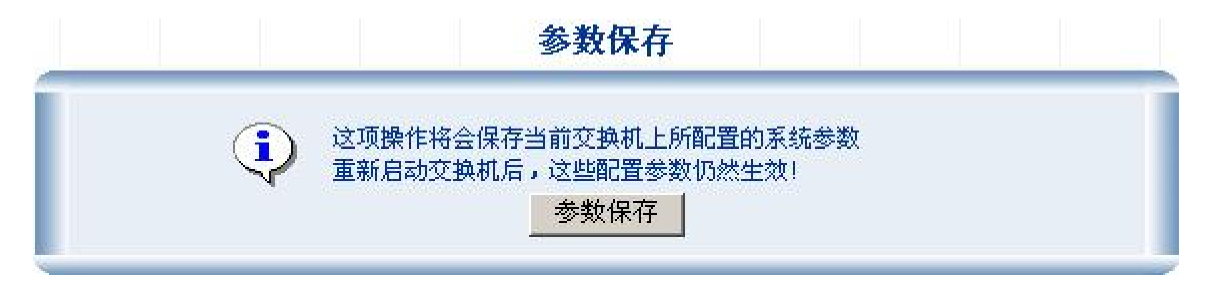


图 6.7

6.1.8 参数备份与恢复

- 参数备份：所有的参数配置好后，用户可以将当前Netcore 7324NSW二四层交换机的配置参数进行备份，方便以后使用。
- 参数恢复：保存了的参数，用户可以任意恢复，点击“浏览”选择备份的参数文件。点

击确定。当“系统参数恢复状态”显示成功时，表示用户参数恢复成功。

参数备份

备份当前交换机的所有参数配置,以便以后的恢复操作

参 数 恢 复	
系统参数文件：	浏览...
系统参数恢复状态：	

确定

图 6.8

6.1.9 恢复缺省参数

恢复Netcore 7324NSW二四层交换机缺省参数配置。

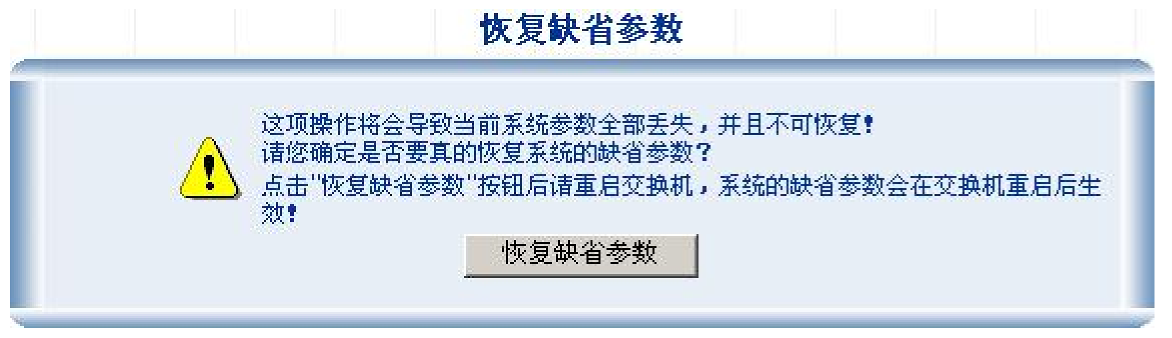


图 6.9


重要提示

此项操作将会导致交换机丢失所有当前保存的参数配置，除非遇到严重的问题，且用尽所有的故障解决方法都无效的情况下。请慎重！

6.1.10 重新启动

将Netcore 7324NSW二四层交换机重新启动。

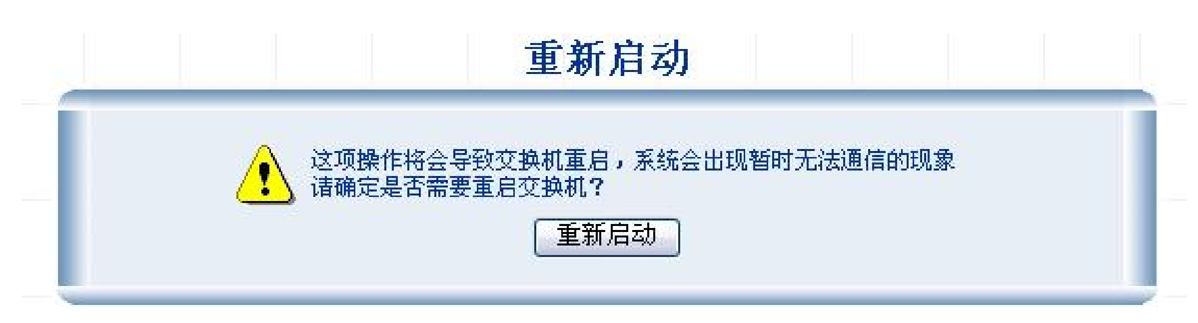


图 6.10

6.2 端口管理

6.2.1 端口配置

用户可以自行根据需要在这里对 Netcore 7324NSW 二四层交换机的各个端口进行配置。

- 端口列表：在“端口列表”框中选择要配置的端口。
- 管理状态：在“管理状态”框中可设定是否打开端口，默认为“Enable”。
- 速度/双工：在“速度/双工”框设定端口传输速度及全双工或半双工，默认为Auto。（暂无1000H模式）
- 流量控制：流量控制功能要求所连接的设备必须支持IEEE 802.3x且可以以全双工的方式传输，当交换机上的缓冲区被存贮满，交换机将发送Pause帧，通知发送方设备暂停发送数据。用户可通过“流量控制”框，来设定是否打开流量控制功能。


友情提示

Auto 是交换机能够自动侦测网络速度、双工状态，并根据网络情况调整自己的传输速率及双工状态以达到最高的传输速率。

端口配置的具体操作：

建议使用默认配置，也可根据情况需要自行配置。在“查看端口状态”项显示交换机当前各端口状态情况（默认配置如下图）



端口	管理状态	连接状态	速度 配置	速度 实际	双工 配置	双工 实际	流量控制 配置	流量控制 实际
Port 1	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 2	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 3	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 4	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 5	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 6	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 7	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 8	Enable	Up	Auto	100M	Auto	Full	Disable	Disable
Port 9	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 10	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 11	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 12	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 13	Enable	Down	Auto	NA	Auto	NA	Disable	NA
Port 14	Enable	Down	Auto	NA	Auto	NA	Disable	NA

图 6.11

6.2.2 端口带宽限制

无论您是哪种接入方式，您都需要合理的整体规划您的带宽，以保证您的带宽最大程度的优化和利用。带宽限制是对交换机入口和出口报文的速率进行控制，使报文以设置的速率进行收发。入口带宽限制通常是为了是报文速率与下游设备相匹配，以避免不必要的报文丢弃和拥塞。

端口带宽限制

入口带宽限制		
注意：如果有网刻，请不要设置带宽限制		
入口端口列表	限制种类	限制带宽 (100Kbps~1000000Kbps)
	Broadcast	Kbps

出口带宽限制	
出口端口列表	带宽(100Kbps~1000000Kbps)
	Kbps

增加

端口	入口限制种类	入口限制带宽(Kbps)	出口限制带宽(Kbps)	删除
1	Broadcast only	N/A	N/A	删除
2	Broadcast only	N/A	N/A	删除
3	Broadcast only	N/A	N/A	删除
4	Broadcast only	N/A	N/A	删除
5	Broadcast only	N/A	N/A	删除
6	Broadcast only	N/A	N/A	删除
7	Broadcast only	N/A	N/A	删除
8	Broadcast only	N/A	N/A	删除
9	Broadcast only	N/A	N/A	删除
10	Broadcast only	N/A	N/A	删除
11	Broadcast only	N/A	N/A	删除
12	Broadcast only	N/A	N/A	删除
13	Broadcast only	N/A	N/A	删除
14	Broadcast only	N/A	N/A	删除
15	Broadcast only	N/A	N/A	删除
16	Broadcast only	N/A	N/A	删除
17	Broadcast only	N/A	N/A	删除
18	Broadcast only	N/A	N/A	删除
19	Broadcast only	N/A	N/A	删除
20	Broadcast only	N/A	N/A	删除
21	Broadcast only	N/A	N/A	删除
22	Broadcast only	N/A	N/A	删除
23	Broadcast only	N/A	N/A	删除
24	Broadcast only	N/A	N/A	删除

图 6.12

- 入口带宽限制：可以设置四种数据包类型



图 6.13

- 出口限制



图 6.14

6.3 冗余与备份

6.3.1 链路聚合原理

链路聚合是将多个端口聚合在一起形成一个汇聚组以实现出/入负荷在各成员端口中的分担同时也提供了更高的连接可靠性。

链路聚合的优点：

- 通过链路聚合，可以在聚合链路的两端获得高带宽。

- 链路聚合提高了链路的可靠性，在一组链路中，如果某条物理链路失效，负载会分配到其他有效物理链路上，虽然可用带宽有所减少，但逻辑链路可以正常工作。

链路聚合应用要求：

- 链路聚合仅用于全双工以太网链路
- 聚合组中的所有链路，必须以同一速率工作
- 不能把聚合端口用于普通连接

6.3.2 Netcore 7324NSW 二四层交换机的链路聚合方式

Netcore 7324NSW二四层交换机共支持设置12个聚合组，每一个聚合组最多包括8个成员端口，设置之后，在端口列表PORT25~PORT36中。


友情提示

端口列表PORT25-PORT36表示8个聚合组。加入了聚合的端口被虚拟成一个端口，该端口的端口号为PORT25-PORT36。

6.3.3 Netcore 7324NSW 二四层交换机的链路聚合配置

在下图中，我们在两台7324NSW二四层交换机上同时设置2个端口聚合，每个端口工作在1000M全双工方式下。这样配置的效果是：得到了一条双向4000M带宽的逻辑链路。

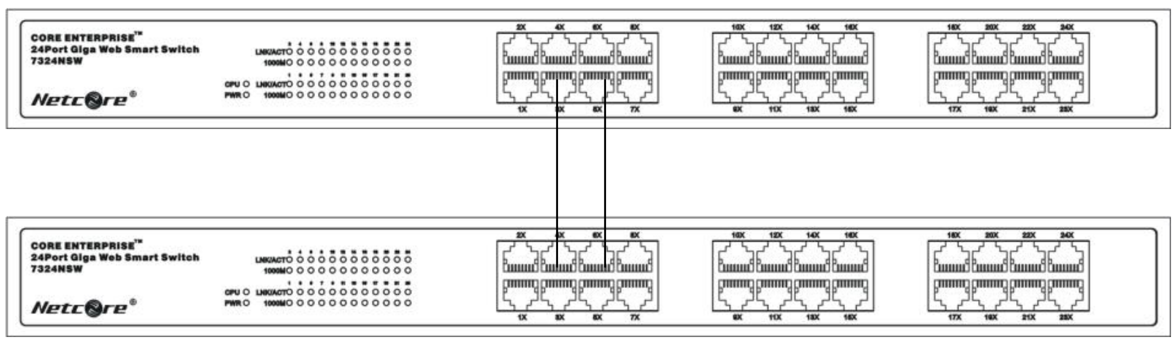


图 6.15


友情提示

Netcore7324NSW二四层交换机支持设置12组聚合组，每组支持添加8个端口

第一步：在“链路聚合”页面中的“聚合组”中选择Port 29。(Port25-36表示为聚合组1-12)

第二步：在交换机A的链路聚合配置中，选择端口列表中的Port3、Port5,单击增加按钮，将Port3、Port5端口加入到聚合组1（Port 29）中。

第三步：在交换机B上重复第二步，将Port3，Port5加入聚合组1（Port29）。如图所示：

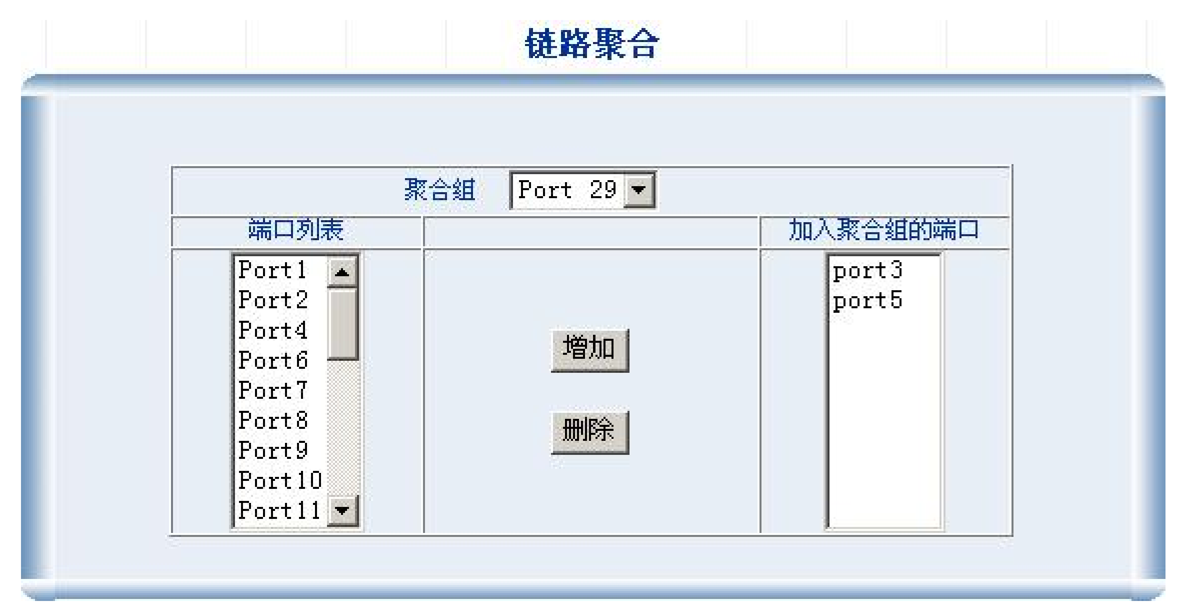


图 6.16

6.4 安全

6.4.1 ACL 配置

6.4.1.1 ACL 的原理

网络设备为了过滤数据包需要配置一系列的匹配规则以识别需要过滤的对象，在识别出特定的对象之后，才能根据预先设定的策略允许或禁止相应的数据包通过。访问控制列表Access Control List (ACL) 就是用来实现这些功能。

ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。ACL 应用在交换机全局或端口，交换机根据ACL中指定的条件来检测数据包从而决定是转发还是丢弃该数据包由ACL 定义的数据包，匹配规则还可以被其它需要对流量进行区分的场合引用如QoS 中流分类规则的定义。

Netcore 7324NS二+四层交换机的ACL条目是由下至上匹配的，基于MAC地址匹配级别高于其他协议类别。

6.4.1.2 ACL 的配置

（1） 基于 MAC 的 ACL 配置

- **ACL 类型**：选择“MAC”
- **源 MAC/目的 MAC**：分别填写源及目的 MAC 地址，如果源 MAC 为空，表示匹配所有的源 MAC 地址，目的 MAC 为空，表示匹配所有的目的 MAC 地址
- **允许/禁止**：PERMIT：允许；DENY：禁止

如果在“允许/禁止”中选择了“PERMIT”（允许）的话，还可以有以下四个可选项进行设定：

* **限流器**：可对本设定的流进行速度的限制
* **统计器**：可对该流进行数据统计，在“网络分析>>QOS 统计器”中进行查看
* **DSCP**：对该流进行 QoS 设定
* **捕获**：可进行限定流的捕获。在 ACL 列表中查看是否开启了捕获，如果开启了，该满足该条件的报文会复制一份发送到 CAPTURE 端口。

添加完毕后点击“增加”以使该条目设置成功。但要使此 ACL 条目生效，需将状态从 Uncommit 转换为 Commit 即可。

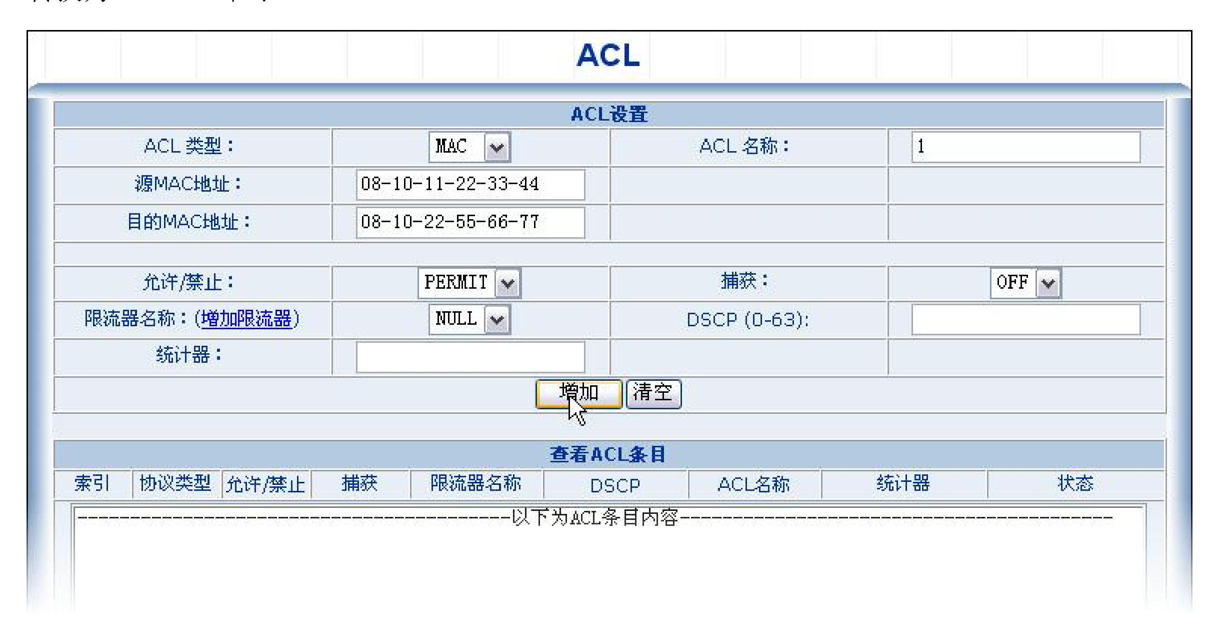


图 6.17



图 6.18

（2） 基于 IP 的设置

* **ACL 类型**：选择“IP”
* **IP 地址及掩码**：IP 地址 ，可以是一个网段，如 192.168.2.0，也可以是一台具体的主机地址，如 192.168.2.161；交换机可根据后面填写的子网掩码来进行判断，如果是 255.255.255.255，那就是一台具体的主机，如果是 255.255.255.0，即是进行了 24 位掩码的匹配。源 IP 和目的 IP 已经不能设为空
* **协议类型**：可根据需要选择，如果是需要所有的请选择“ANY”
* **允许/禁止**：PERMIT：允许；DENY：禁止

如果在“允许/禁止”中选择了“PERMIT”（允许）的话，还可以有以下四个可选项进行设定：

* **限流器**：可对本设定的流进行速度的限制
* **统计器**：可对该流进行数据统计，在“网络分析>>QOS 统计器”中进行查看
* **DSCP**：对该流进行 QoS 设定
* **捕获**：可进行限定的 IP 流的捕获。在 ACL 列表中查看是否开启了捕获，如果开启了，该满足该条件的报文会复制一份发送到 CAPTURE 端口。

添加完毕后点击“增加”以使该条目设置成功。但要使此 ACL 条目生效，需将状态从 Uncommit 转换为 Commit 即可。

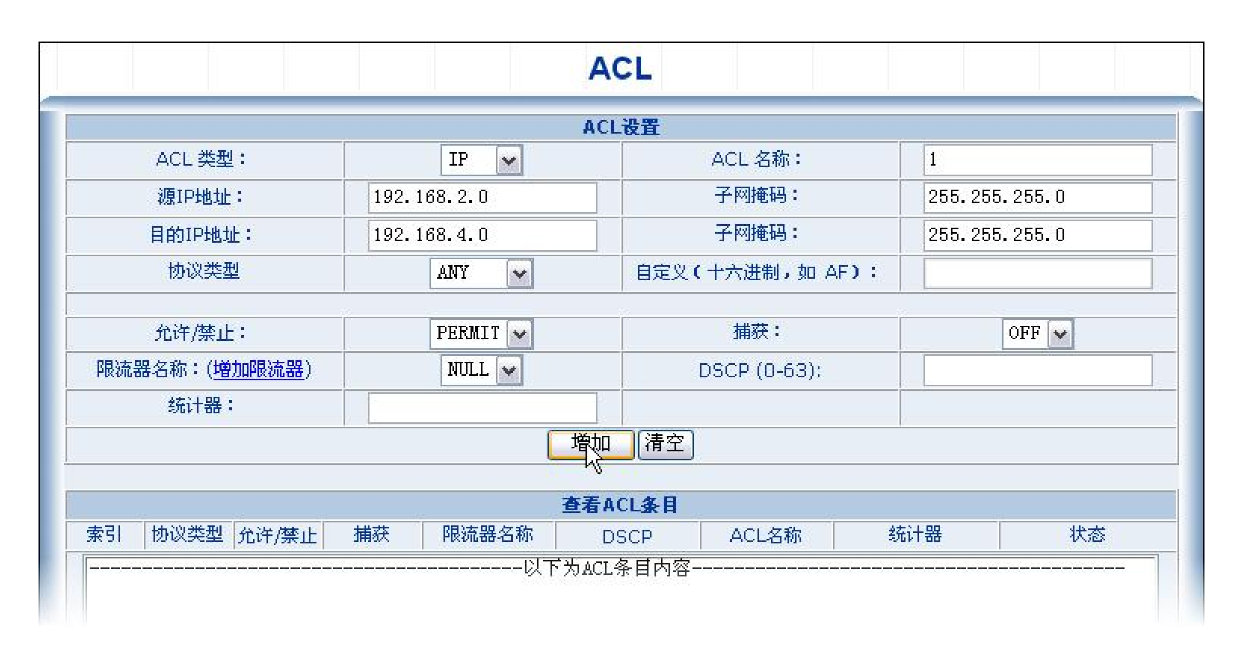


图 6.19



图 6.20

（3） 基于 TCP、UDP 的 ACL 设定

- **ACL 类型：**选择“TCP”或“UDP”
- **IP 地址即掩码：**IP 地址 ，可以是一个网段，如 192.168.2.0，也可以是一台具体的主机地址，如 192.168.2.161；交换机可根据后面填写的子网掩码来进行判断，如果是 255.255.255.255，那就是一台具体的主机，如果时 255.255.255.0，即是进行了 24 位掩码的匹配。源 IP 和目的 IP 已经不能设为空
- **源、目的端口：**分别为 TCP 或者 UDP 中的源和目的端口
- **允许/禁止：**PERMIT：允许；DENY：禁止

如果在“允许/禁止”中选择了“PERMIT”（允许）的话，还可以有以下四个可选项进行设定：

- ＊ **限流器：**可对本设定的流进行速度的限制
- ＊ **统计器：**可对该流进行数据统计，在“网络分析>>QOS 统计器”中进行查看
- ＊ **DSCP：**对该流进行 QoS 设定
- ＊ **捕获：**可进行限定 TCP 或 UDP 流的捕获。在 ACL 列表中查看是否开启了捕获，如果开启了，该满足该条件的报文会复制一份发送到 CAPTURE 端口。

添加完毕后点击“增加”以使该条目设置成功。但要使此 ACL 条目生效，需将状态从 Uncommit 转换为 Commit 即可。

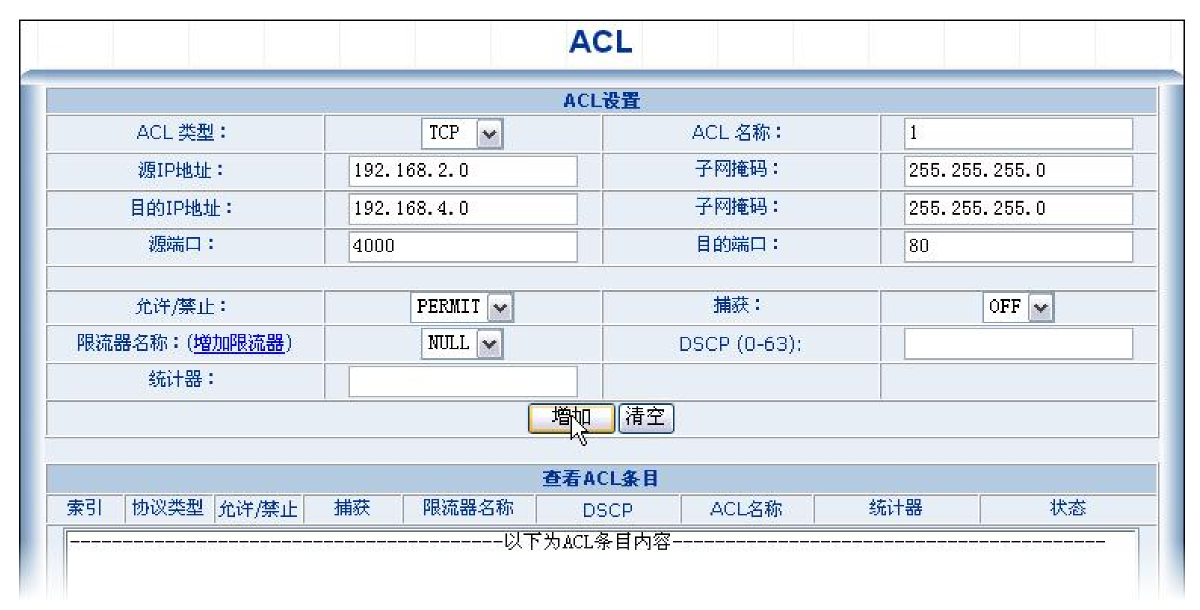


图 6.21



图 6.22

（4） 基于 ICMP 的 ACL 设置

- **ACL 类型**：选择“ICMP”
- **IP 地址即掩码**：IP 地址 ，可以是一个网段，如 192.168.2.0，也可以是一台具体的主机地址，如 192.168.2.161；交换机可根据后面填写的子网掩码来进行判断，如果是 255.255.255.255，那就是一台具体的主机，如果时 255.255.255.0，即是进行了 24 位掩码的匹配。源 IP 和目的 IP 已经不能设为空
- **允许/禁止**：PERMIT：允许；DENY：禁止

  如果在“允许/禁止”中选择了“PERMIT”（允许）的话，还可以有以下四个可选项进行设定：

  * **限流器**：可对本设定的流进行速度的限制
  * **统计器**：可对该流进行数据统计，在“网络分析>>QOS 统计器”中进行查看
  * **DSCP**：对该流进行 QoS 设定
  * **捕获**：可进行限定 ICMP 流的捕获。在 ACL 列表中查看是否开启了捕获，如果开启了，该满足该条件的报文会复制一份发送到 CAPTURE 端口。

添加完毕后点击“增加”以使该条目设置成功。但要使此 ACL 条目生效，需将状态从 Uncommit 转换为 Commit 即可。

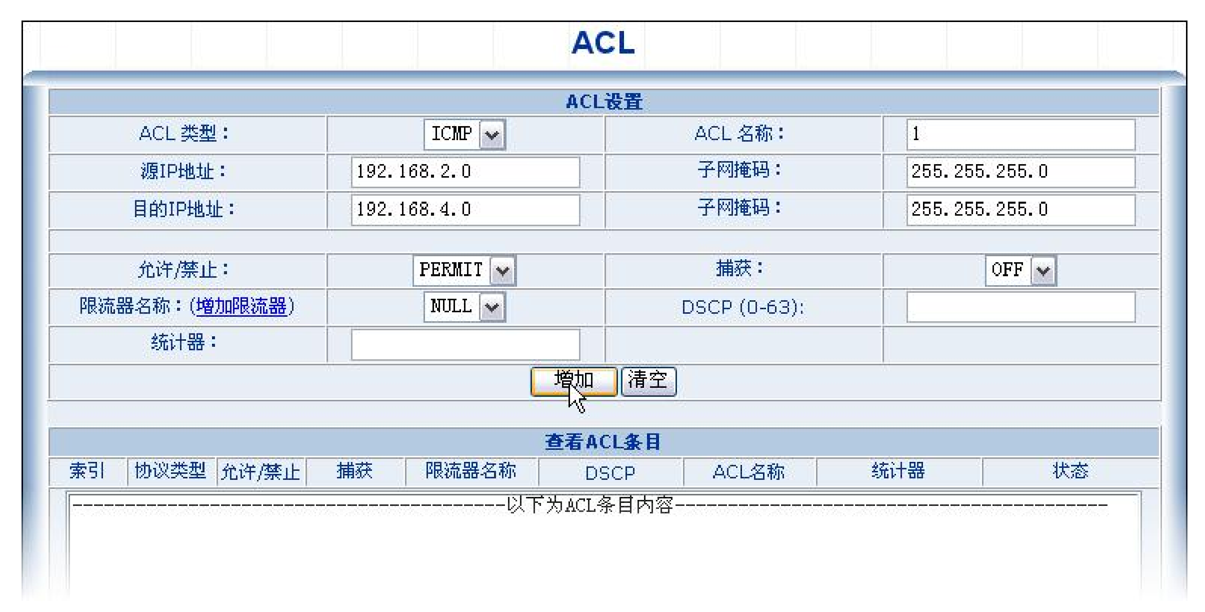


图 6.23



图 6.24

6.4.1.3 ACL 的查看、删除、条目优先级调整、状态

（1） ACL 条目的查看

在 ACL 配置页面选中您需要查看的条目，点击查看，则可查看到具体的配置

ACL

配置ACL			
ACL类型：	IP	ACL名称：	
源IP地址：	192.168.2.0	子网掩码：	255.255.255.0
目的IP地址：	192.168.4.0	子网掩码：	255.255.255.0
协议类型：	ANY	自定义（十六进制，如 AF）：	
允许/禁止：	PERMIT	捕获：	OFF
限流器名称：（增加限流器）	NULL	DSCP (0-63)：	

增加 清空

查看ACL条目

索引	协议类型	允许/禁止	捕获	限流器名称	DSCP	ACL名称	状态

---以下为ACL条目内容---
-1--------IP-------PERMIT-----------OFF-----------N/A----------N/A-------N/A-------UNCOMMIT---

查看 上移 下移 删除 COMMIT

图 6.25

（2） ACL 条目的删除

选中你所想删除的条目，点击删除。而删除 ACL 条目不管其状态是否 COMMIT，该功能会直接从硬件上删除该条 ACL 配置。

（3） ACL 条目的优先级调整（基础优先级协议不变，并且调整 ACL 优先级不会改变条目是否 COMMIT 的状态。）

选中你所想移动的条目，点击“上移”或“下移”。

（4） ACL 条目的状态

Uncommit:条目设置成功，但功能并没有生效。

Commit：条目设置成功，并已经生效。

6.4.1.4 流量整行（增加限流器）

流量整形是对输出报文的速率进行控制，使报文以均匀的速率发送出去。流量整形通常是为了是报文速率与下游设备相匹配，以避免不必要的报文丢弃和拥塞。它和流量监管的主要区别在于流量整形是缓存超过速率限制的报文，使报文以均匀的速率发送出去，而流量监管则是丢弃超过流量速率限制的报文。但是流量整形会增加延迟，而流量监管不会引入额外的延迟。

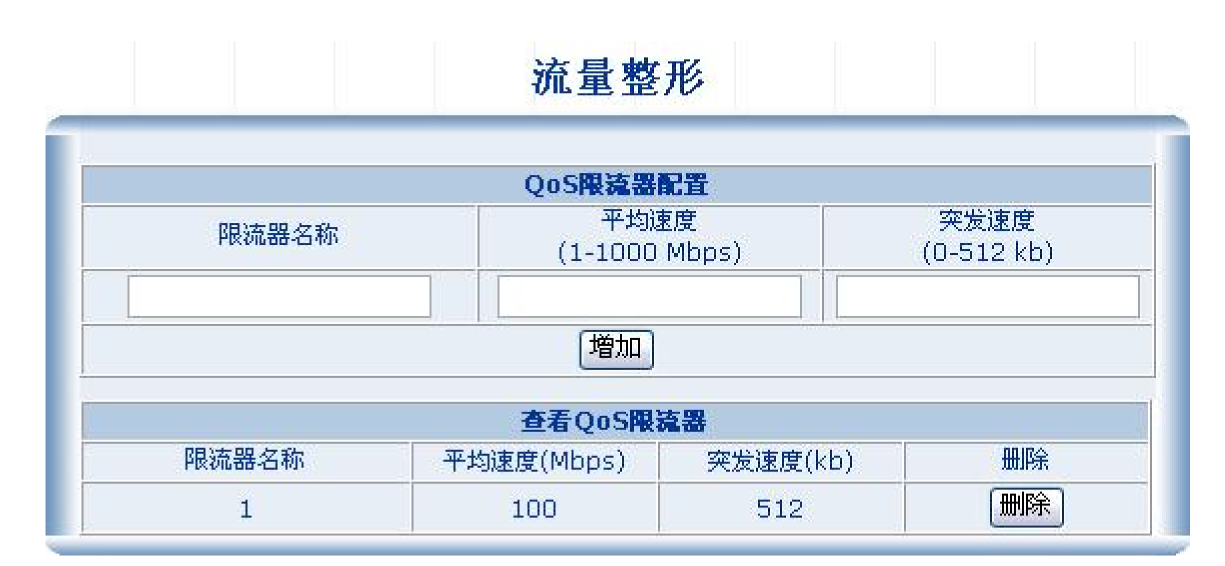


图 6.26

6.4.2 安全防御

交换机里可以通过两种方式来进行安全防御的设置。



图 6.27

- 模板形式：内嵌在网络环境中常见的病毒攻击



图 6.28

- 手动设置：根据所处环境，所需情况自行设置

用户定义安全防御	
名称:	1
协议:	☑TCP ☑UDP
TCP端口:	133
UDP端口:	133
确定	

图 6.29

6.4.3 ARP 攻击防御

该设置用于定时发送路由器Arp Response，以保护没有直接连接本交换机的主机到路由器的连通性。在此指的路由器，可能是属性为路由器的主机。要修改主机的属性为路由器，请参看图6.81。

ARP攻击防御

说明：该设置用于定时发送路由器Arp Response，以保护没有直接连接本交换机的主机到路由器的连通性。最多支持6台路由器。（填0表示取消设置）

注意：在PortBased VLAN和IEEE 802.1Q VLAN之间切换后，请重设此功能。

ARP攻击防御保护时间(10-3000ms):

确定

图 6.30

6.4.4 VLAN 配置

6.4.4.1 VLAN（Virtual Local Area Network）的原理

它是一种通过将局域网内的设备逻辑地(而不是物理地)划分成一个个网段，从而实现虚拟工作组的技术。为了建立起安全的、独立的广播域或者组播域，可以将交换机上的端口组合成多个虚拟局域网（VLAN）。设置VLAN的主要目的是为了限制广播包的传播范围和降低广播包的影响。所有以太网数据包，如单播（unicast）、组播（multicast）、广播（broadcast），以及未知（unknown）的数据包，都将只在VLAN内传送。这样在一定程度上，可以提高网络的安全性。

VLAN的另一个优点是可以改变网络的拓扑结构，但并不需要网络中的工作站发生物理上的移动或者网络线路连接上的变动。可以仅仅改动工作站的VLAN设置，就可将工作站从一个VLAN（如销售部VLAN）“移到”了另一个VLAN（市场部VLAN）这可使网络节点的移动、变换、增加变得非常灵活和容易。

Netcore 7324NSW 交换机上支持两种VLAN：Port Based VLAN、802.1Q的VLAN。但在交换机上任何时刻都只能激活一种VLAN。这样，你需要选择一种最适合你的网络环境的VLAN类型

来设置交换机。

IEEE 802.1QVLAN的去标记特性（untagging）使得它可以与所有合法的、无法识别VLAN标记（VLANtag）的交换机或网卡在一起工作。而IEEE802.1Q延伸到多个兼容IEEE 802.1Q的交换机上。

- Port Based VLAN

基于端口（port-based）的VLAN是一种简化的802.1QVLAN。基于端口的VLAN的理解和实现非常简便，如果网络管理员想快速且简易地设置VLAN，以限制广播包在网络上的传输，可选择这种最简单的基于端口的VLAN划分方法。

为了能可靠地执行VLAN的设置，请确保设备都已经直接连接在交换机上。如果是通过一台HUB、交换机或其它中继器将节点连接到交换机的端口上的，连接在该HUB、交换机或其它中继器上的所有节点都将成为该VLAN的成员。

如果想设置基于端口的VLAN，只需为其选择一个VLAN ID（交换机所有端口缺省的VID都为1），并为VLAN起一个名字，指定哪些端口属于这个VLAN就可以了，其余的端口将被自动地隔离在外。



友情提示

Netcore7324NSW交换机支持49个port-based VLAN。

- 802.1Q的VLAN

802.1Q协议，即Virtual Bridged Local Area Networks协议，主要规定了VLAN的国际标准，内容是一种在逻辑上划分网络桥接的局域网结构,并提供定义用户组在跨越不同交换设备VLAN之间的连接服务，这使得不同厂商之间的VLAN互通成为可能。VLAN的最大数目也不受交换机端口数目的限制，最大可达到4094个。

在802.1QVLAN中，网卡（NIC）不必去识别数据包头部分的802.1Q标记（tag），网卡只需发送和接收普通的以太网数据包。TAG的信息由交换机的端口根据相应的PVID加入到数据包中。交换机根据包头中的TAG信息决定如何转发这个数据包。

在理解IEEE 802.1QVLAN时，有两个非常重要的名词需要掌握，就是端口VLAN的ID（Port VLANID numbers 简写为PVID）和VLAN的ID（VLANID numbers 简写为VID）。这两个变量都是定义在端口上的，但是两者间有很大的区别。用户可以仅为每个交换机端口定义一个PVID。PVID 定义了交换机将向哪一个VLAN转发数据包，以及什么时候数据包会需要转发到另一台交换机的端口上，或者网络中的某个地方。另外，用户也可以定义某个端口同时属于多个VLAN（即VIDs），使得它可以接收网络中多个VLAN的数据包。PVID 和VID 这两个变量用于控制端口发送和接收VLAN数据流的能力，而两者之间的区别在于后者还允许信息可以在多个VLAN间共享。



友情提示

Netcore7324NSW二四层交换机支持512个802.1Q VLAN。

6.4.4.2 VLAN 的相关术语

- Tagging

将802.1QVLAN的信息加入数据帧头。具有加标记能力的（tagging enabled）端口会将PVID、优先级和其它VLAN信息加入到所有进出该端口的数据帧中。如果在此前数据包已经被做过标

记，端口将不对该数据包进行改动，让其保持其已有的VLAN信息。标记（Tagging）使得数据包能够从一台支持802.1Q的交换机能够传送到另一台同类的交换机上。

- Untagging

将802.1QVLAN的信息从数据帧头去掉。具有去标记能力的（untagging enabled）端口会将VID、优先级和其它VLAN信息从所有进出该端口的数据包包头中去掉。如果在此前数据包内没有被标记过,端口将不对该数据包进行改动。去标记（Untagging）使得数据包能够从一台支持802.1Q的交换机传送到其它不支持802.1Q的交换机上。

- Access 链路

即Untagging，是将802.1QVLAN的信息从数据帧头去掉。具有去标记能力的（untagging enabled）端口会将VID、优先级和其它VLAN信息从所有出该端口的数据包包头中去掉。如果在此前数据包内没有被标记过,端口将不对该数据包进行改动。去标记（Untagging）使得数据包能够从一台支持802.1Q的交换机传送到其它不支持802.1Q的交换机上。

- Trunk 链路

是将某端口设定为对某一个VLAN的数据帧Untagging，而对其他您所选定的VLAN的数据帧Tagging，Tagging是将802.1QVLAN的信息加入数据帧头。具有加标记能力的（tagging enabled）端口会将PVID、优先级和其它VLAN信息加入到所有进出该端口的数据帧中。如果在此前数据包已经被做过标记，端口将不对该数据包进行改动，让其保持其已有的VLAN信息。标记（Tagging）使得数据包能够从一台支持802.1Q的交换机能够传送到另一台同类的交换机上。

- PVID

是端口所属的VID号。

6.4.4.3 Netcore 7324NSW 二四层交换机的 VLAN 设置方法

6.4.4.3.1 Netcore 7324NSW 二四层交换机的 VLAN 基本设置方法

- Port Based VLAN

下列操作设置图例中的Port-based VLAN。如图所示，将Netcore7324NSW交换机的1~4端口设为VLAN2，5~8端口为VLAN3。

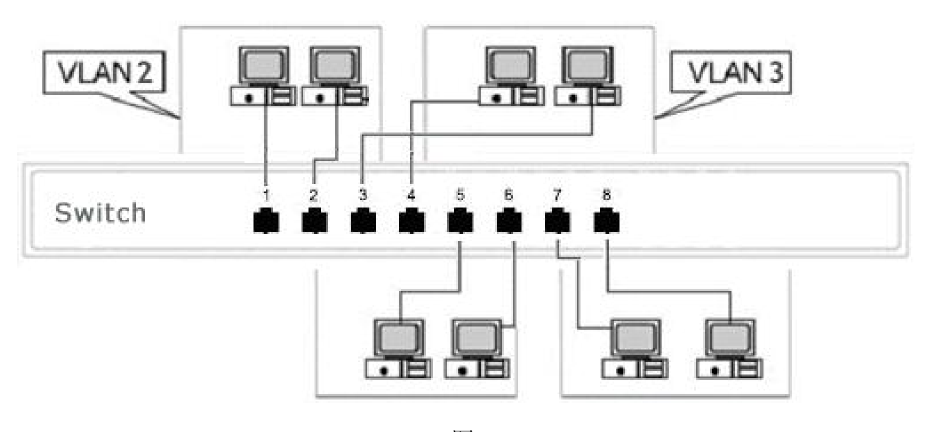


图 6.31

第一步：在VLAN配置中选中使用“port-based VLAN”点击确定。



图 6.32

第二步："port-based VLAN"配置页面中点击"增加/修改"按钮。



图 6.33

友情提示

上图所示的VLAN1是交换机的默认VLAN/"Default VLAN" VID=1。在初始情况下交换机的所有端口都属于default VLAN，当该端口加入新的VLAN时，自动从default VLAN中删除。

第三步：现在开始进行将Netcore7324NSW交换机的1~4端口设为VLAN1，5~8端口为VLAN2的设置。在"VLAN名称"框输入VLAN2、"VID"框输入2，然后点击"确定"。然后选中"port1"~"port4"点击"增加"将端口加入VLAN2。



图 6.34

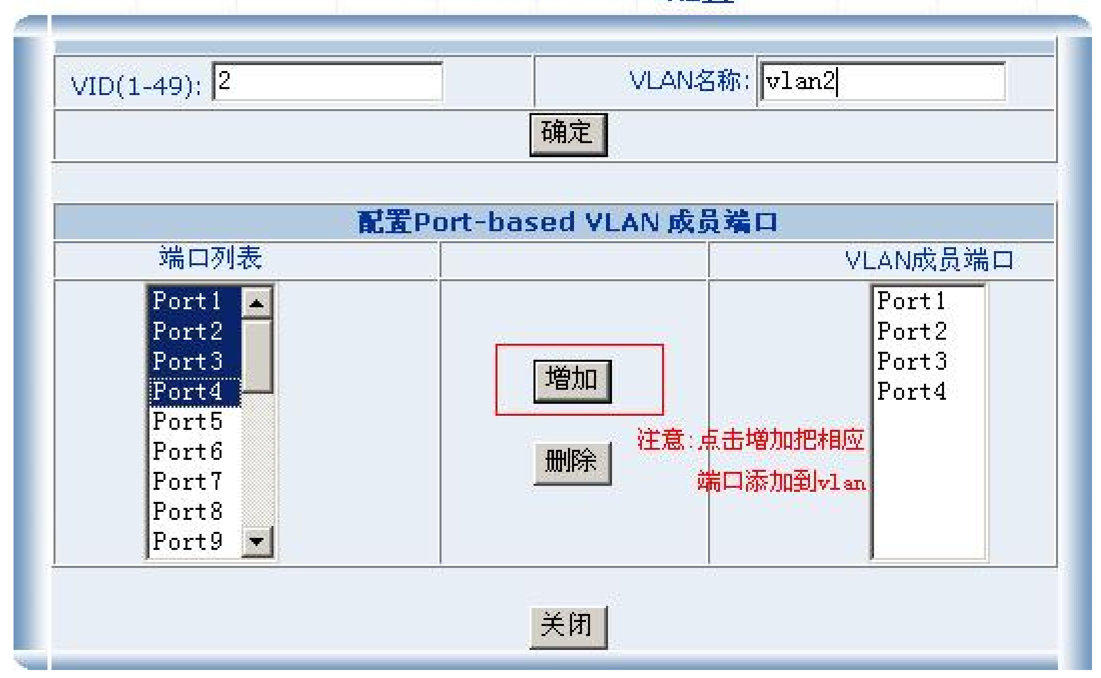


图 6.35

第四步：返回“图6.33”所示页面，点击“查看 VLAN成员” 可以看到已成功设置了VLAN2。



图 6.36

友情提示

port1-port4添加到VLAN2后，交换机自动从VLAN1中删除了port1-port4 四个端口

将“port5”~“port8”加入VLAN3的步骤同上类似。

第五步：返回“port-based VLAN”配置页面中点击Vlan名称可以进行修改Vlan配置，如下图所示。



图 6.37

- 802.1QVLAN

在支持802.1Q的交换机(802.1Q-compliant switches)之间的数据传送原理，如下图所示。

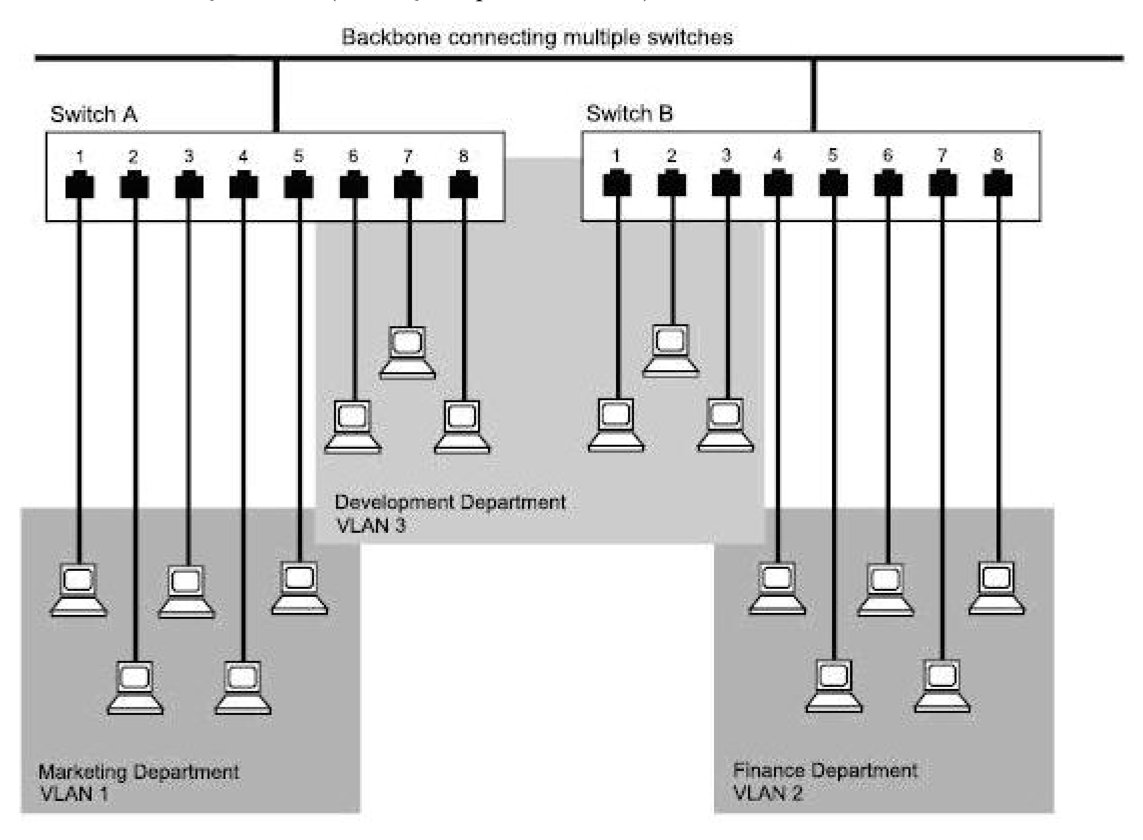


图 6.38

结合上图在Netcore7324NSW二四层交换机上的具体操作：

第一步：您可以看到所有端口的VLAN信息显示。

802.1Q VLAN

端口	链路类型	PVID	出口规则
Port1	Access	1	Untagged=1
Port2	Access	1	Untagged=1
Port3	Access	1	Untagged=1
Port4	Access	1	Untagged=1
Port5	Access	1	Untagged=1
Port6	Access	1	Untagged=1
Port7	Access	1	Untagged=1
Port8	Access	1	Untagged=1
Port9	Access	1	Untagged=1
Port10	Access	1	Untagged=1
Port11	Access	1	Untagged=1
Port12	Access	1	Untagged=1
Port13	Access	1	Untagged=1

图 6.39

交换机的802.1Q的配置是基于每一个端口来配置所属VLAN的信息，首先按第三步进入端口配置该端口所属VLAN信息。

第三步：点击您所需要设定的端口，进入设置页面。

802.1Q VLAN

端口	链路类型	PVID	出口规则
Port1	Access	1	Untagged=1 <--点击此处可以修改该端口的Vlan配置
Port2	Access	1	Untagged=1
Port3	Access	1	Untagged=1
Port4	Access	1	Untagged=1
Port5	Access	1	Untagged=1
Port6	Access	1	Untagged=1
Port7	Access	1	Untagged=1
Port8	Access	1	Untagged=1
Port9	Access	1	Untagged=1
Port10	Access	1	Untagged=1
Port11	Access	1	Untagged=1
Port12	Access	1	Untagged=1
Port13	Access	1	Untagged=1

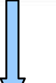


图 6.40

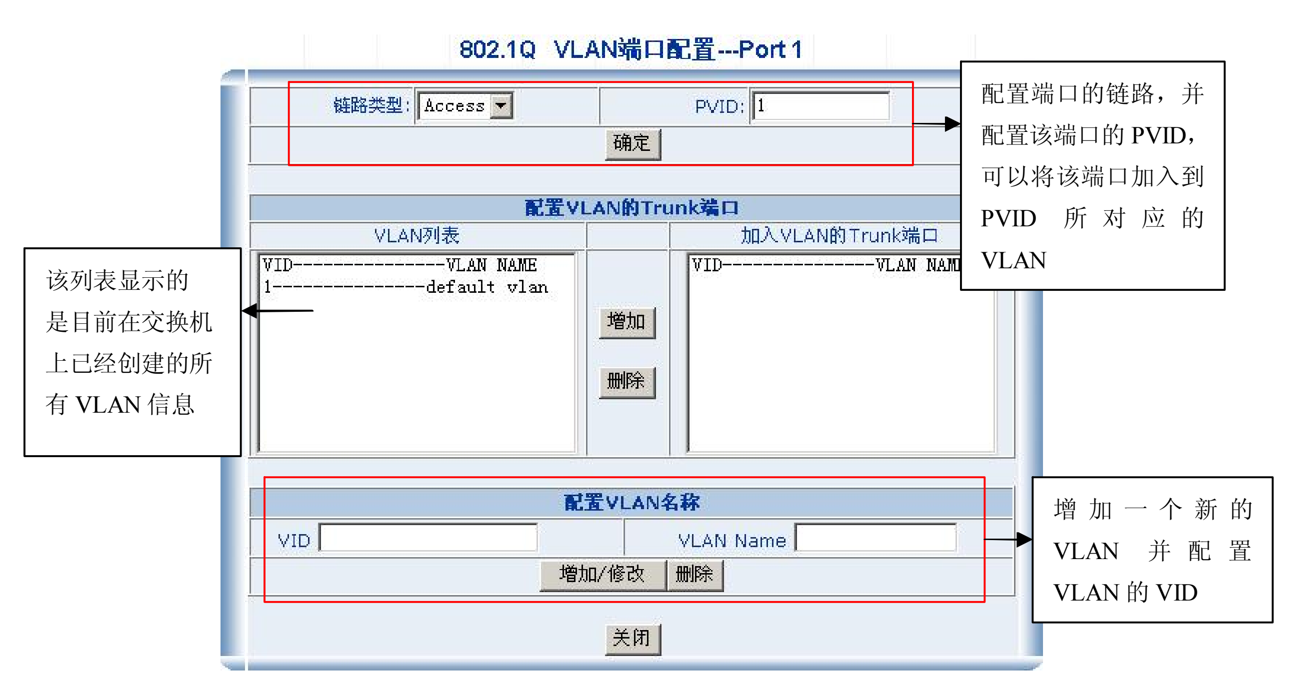


图 6.41


友情提示

上图所示的VLAN1是交换机的默认VLAN/“Default VLAN” VID=1。在初始情况下交换机的所有端口都属于default VLAN，当该端口加入新的VLAN时，自动从default VLAN中删除。

第四步：增加一个新的VLAN

增加VLAN。输入VLAN名称，输入VID的值，



图 6.42

新增加的VLAN会显示在VLAN列表中



图 6.43

增加了VLAN后，可以对应每个端口的配置，通过配置PVID和Trunk 端口属性，决定是否将该端口加入一个VLAN 。

第五步：将端口加入一个VLAN

- **配置PVID**：通过配置PVID，将端口加入一个VLAN


友情提示
交换机默认将 PVID 与 VID 与 VLAN 对应。PVID=2 相当于将一个端口设置为 VLAN2 的成员。

例如：将端口2的链路设置为ACCESS，并将port2的PVID设置为2 ，此时已经将端口2配置为VLAN2的成员



图 6.44

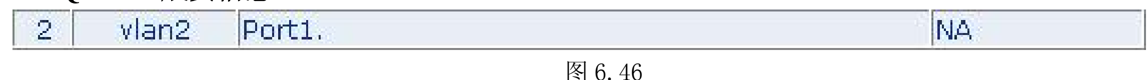
- **配置VLAN的Trunk端口**
- 在VLAN列表中选择您从该端口需要Tagging的VLAN（选中表明已经将端口加入到某个VLAN），增加到右边的“加入VLAN的Trunk端口”列表中。如果端口属于多个VLAN，没有选中的VLAN的从该端口出去时都不带tag头。

例如：选中VLAN2。，从该端口出去的VLAN2数据都必须带Tag头。



图 6.45

第六步：返回图6.17所示页面，点击“查看VLAN成员”，查看该交换机二层交换机的802.1QVLAN成员信息。



2	vlan2	Port1.	NA

图 6.46

例：PC1与PC3属于同一VLAN ；PC2与交换2上某一台机器属于同一VLAN

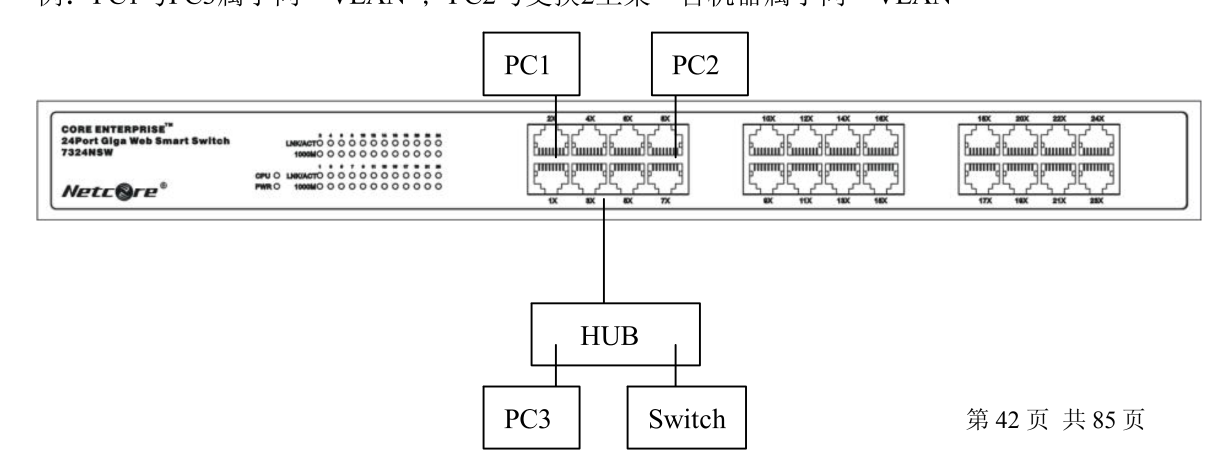


图 6.47

分析：根据需求需要创建两个VLAN ：VLAN2和VLAN3 ，假设PC1在Port1上；PC2 在port3上，HUB接在Port2上。需要将端口1、2加入VLAN2；将端口2、3加入VLAN3（端口2既属于VLAN2又属于VLAN3）。并且让从端口2出去的VLAN2的数据Untagging（因为PC只能接受不带tag头的包）对VLAN3的数据tagging，也就是将Port2的链路设置为Trunk链路，即要传输带tag的包又要传输不带tag头的包。

- 首先创建VLAN2和VLAN3

配置VLAN名称

VID 2 VLAN Name Vlan2

增加/修改 删除

图 6.48

创建VLAN3类似。

- 配置端口1

将端口1配置为VLAN2，将端口1的PVID设置为2 ，系统会自动加端口1加入VLAN2 ，因为端口1直接接PC，链路应该设置为Access

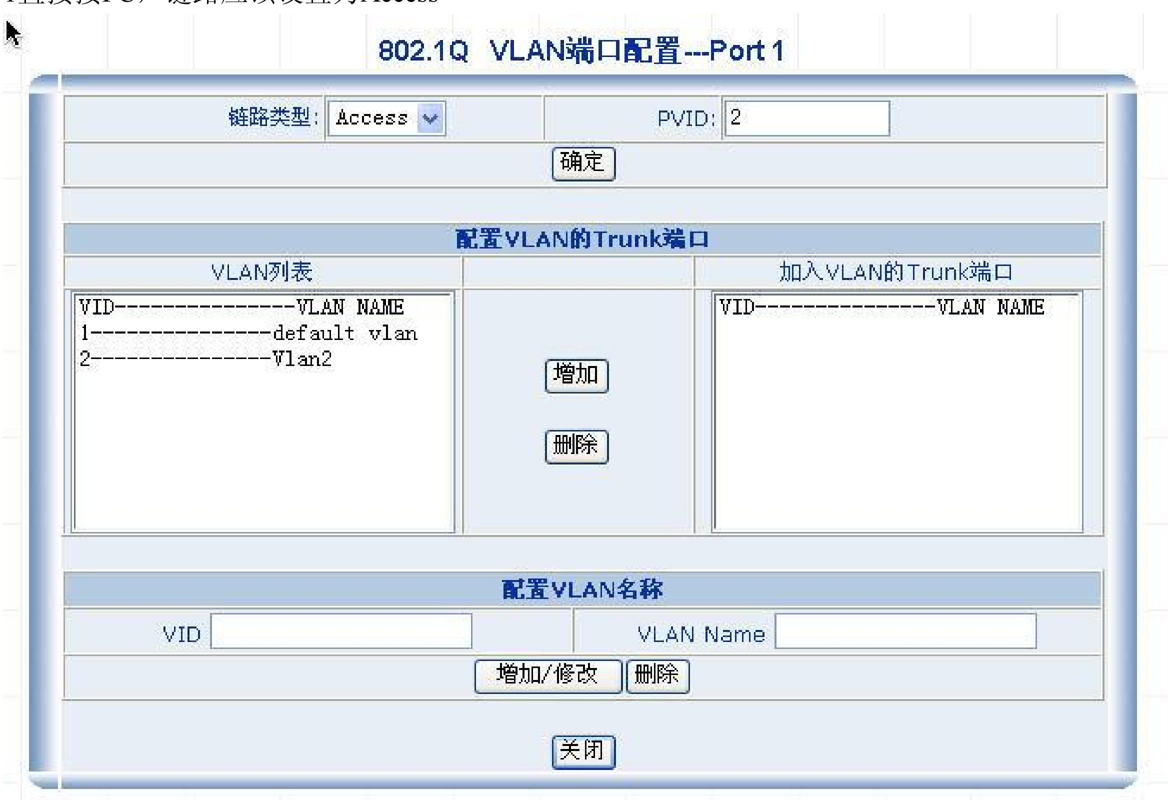


图 6.49

- 配置端口3

将端口3配置为VLAN3，就是将端口3的PVID设置为3 ，系统会自动加端口3加入VLAN3 ，因为端口3直接接PC，链路应该设置为Access

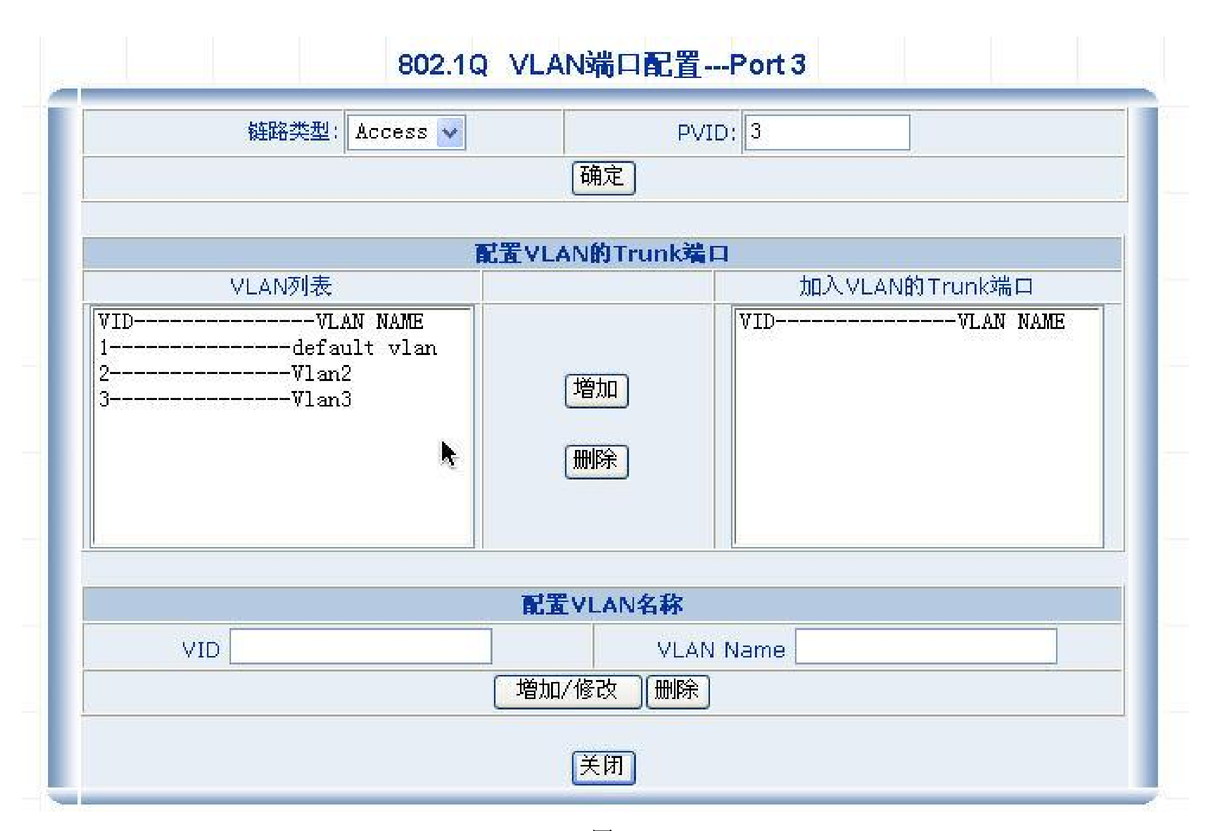


图 6.50

- 配置端口2

  先将链路类型设置为Trunk。再配PVID，由于端口2同属于VLAN2和VLAN3，那么PVID应该怎么配呢？如果将PVID配置成2 ，那么系统会自动将从该端口出去的VLAN2的数据都不带tag头，而需求要求VLAN的数据是不能带tag头的，所以将PVID配置成2。需求要求VLAN3的数据要带tag，那么需要在“配置VLAN的Trunk端口”中选中VLAN3。这样VLAN3的数据从端口2出去时是带tag的数据。

802.1Q VLAN端口配置---Port 2

链路类型: Trunk　PVID: 2

确定

配置VLAN的Trunk端口

VLAN列表		加入VLAN的Trunk端口
VID---------------VLAN NAME 1---------------default vlan 2---------------Vlan2 3---------------Vlan3	增加 删除	VID---------------VLAN NAME 3---------------Vlan3

配置VLAN名称

VID　VLAN Name

增加/修改　删除

关闭

图 6.51

配置完成后可以去查看所有VLAN的配置信息



802.1Q VLAN

端口	链路类型	PVID	出口规则
Port1	Access	2	Untagged=2
Port2	Trunk	2	Untagged=2,Tag=3,
Port3	Access	3	Untagged=3
Port4	Access	1	Untagged=1
Port5	Access	1	Untagged=1
Port6	Access	1	Untagged=1
Port7	Access	1	Untagged=1

图 6.52

再查看VLAN的成员列表



查看VLAN成员

VID	VLAN名称	VLAN成员	VLAN Trunk端口
1	default vlan	Port4.Port5.Port6.Port7.Port8.Port9.Port10.Port11.Port12.Port13.Port14.Port15.Port16.Port17.Port18.Port19.Port20.Port21.Port22.Port23.Port24.Port25.Port26.Port27.Port28.	NA
2	Vlan2	Port1.Port2.	NA
3	Vlan3	Port2.Port3.	Port2.

关闭

图 6.53

6.4.4.3.2 Netcore 7324NSW 二四层交换机的 VLAN 新增功能设置方法

802.1Q VLAN中新增的一个Always Untag的功能，可以实现port-base VLAN的功能。

802.1Q VLAN端口配置---Port 1

链路类型: Always Untag
Access
Trunk
Always Untag
PVID: 1
确定

配置VLAN的Trunk端口
VLAN列表
加入VLAN的Trunk端口
VID---------------VLAN NAME
1---------------default vlan
增加
删除
VID---------------VLAN NAME

配置VLAN名称
VID
VLAN Name
增加/修改
删除
关闭

图 6.54

下面具体应用来说明此功能：

- 目前有一些应用，将局域的划分为几个 VLAN，让各自 VLAN 中的机器不能互相访问，但是网络中有一台公用的服务器，所有设备又都能访问服务器。

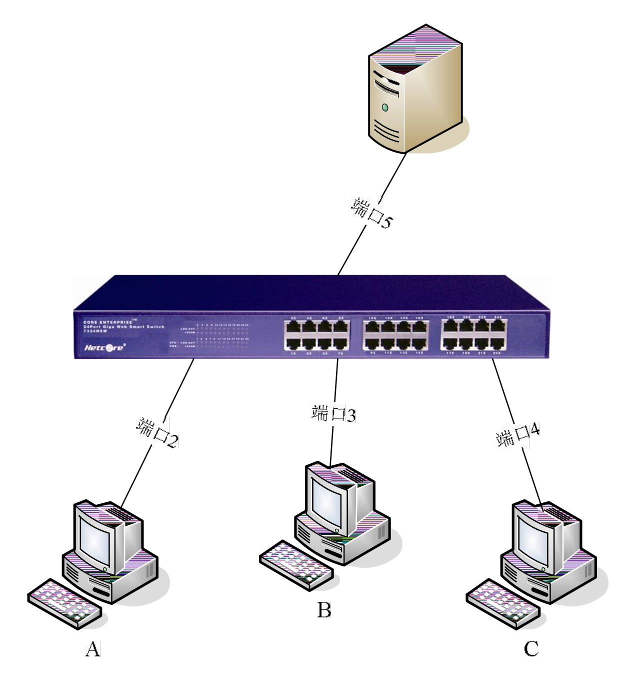


图 6.55

上图中，主机 A、B、C 分别位于交换机 2、3、4 端口，服务器接在 5 号端口。要实现 A、B、C 不能互相访问，但又能同时访问服务器，我们应该怎么设置 VLAN 呢？

配置思路：

需要配置四个 VLAN

VLAN	成员端口
VLAN2	2、5
VLAN3	3、5
VLAN4	4、5
VLAN5	2、3、4、5

端口	PVID
5	5
2	2
3	3
4	4

1、建立 VLAN2、VLAN3、VLAN4、VLAN5

2、端口 2 的配置方法：

将 port2 的 PVID 设置为 2

将链路类型设置为：Always untag

将端口 2 加入到 VLAN5 中

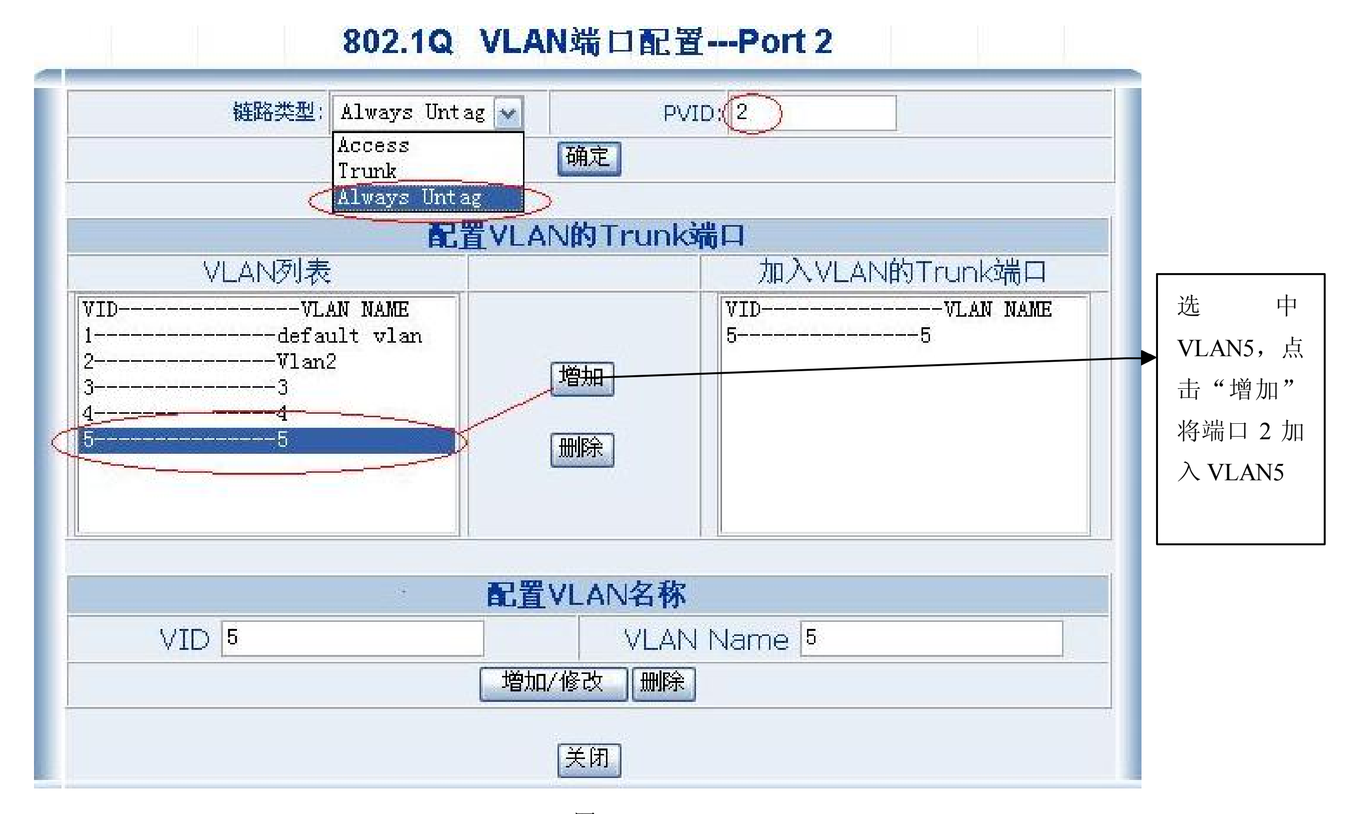


图 6.56

3、端口 3 的配置方法：

将 Port 3 的 PVID 值设置为 3

链路类型为：Always untag

将端口 3 加入到 VLAN5 中

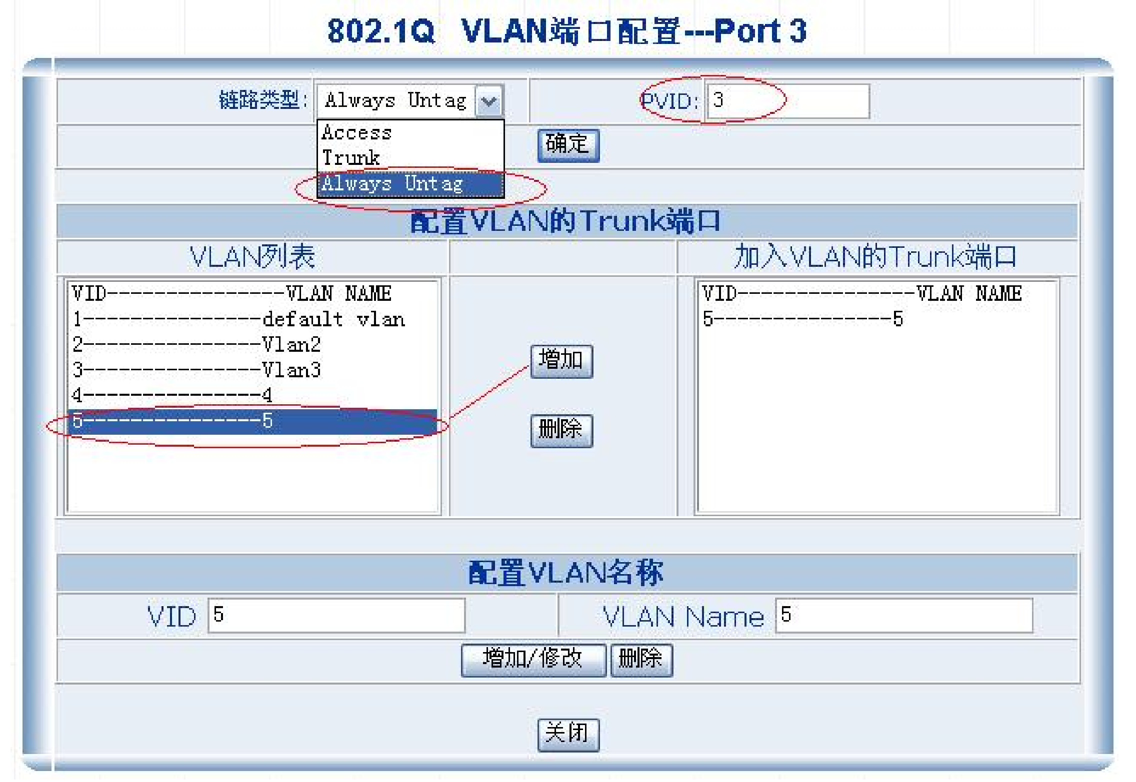


图 6.57

4、端口 4 的配置方法：
将 Port 4 的 PVID 值设置为 4
链路类型为：Always untag
将端口 4 加入到 VLAN5 中

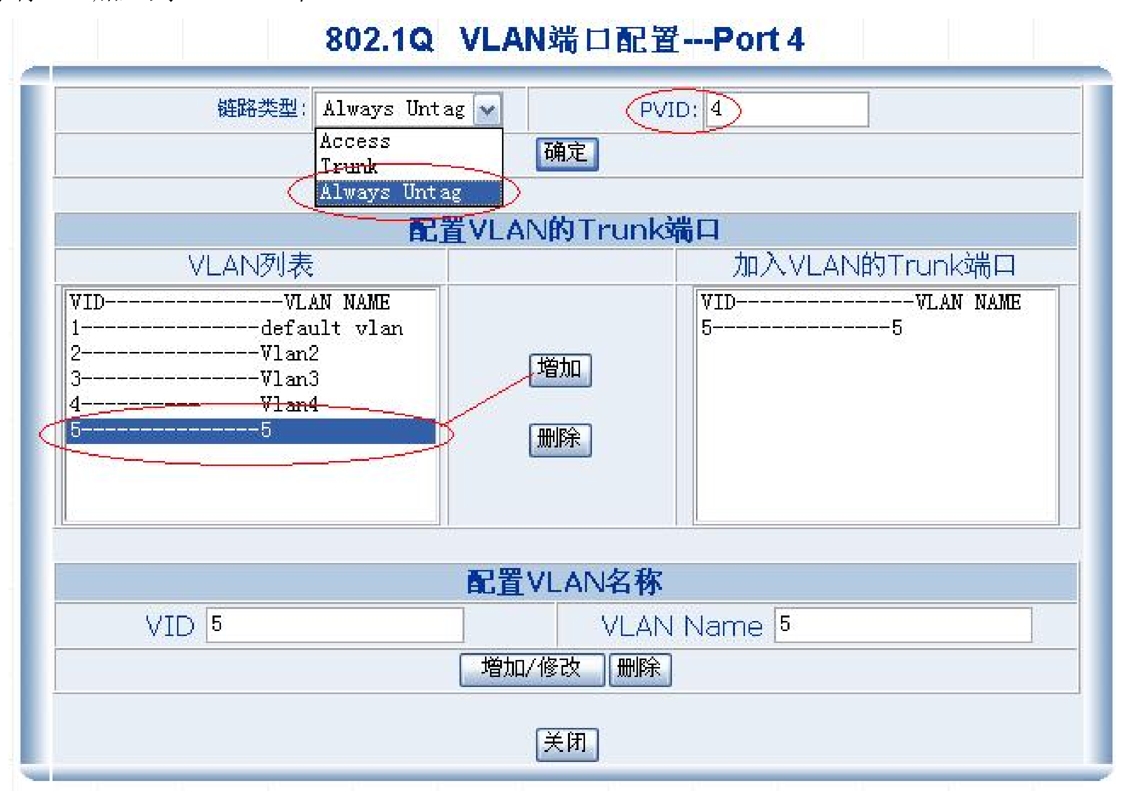


图 6.58

5、端口 5 的配置方法：
将 Port 5 的 PVID 值设置为 5
链路类型为：Always untag
将端口 5 加入到 VLAN2、VLAN3、VLAN4 中

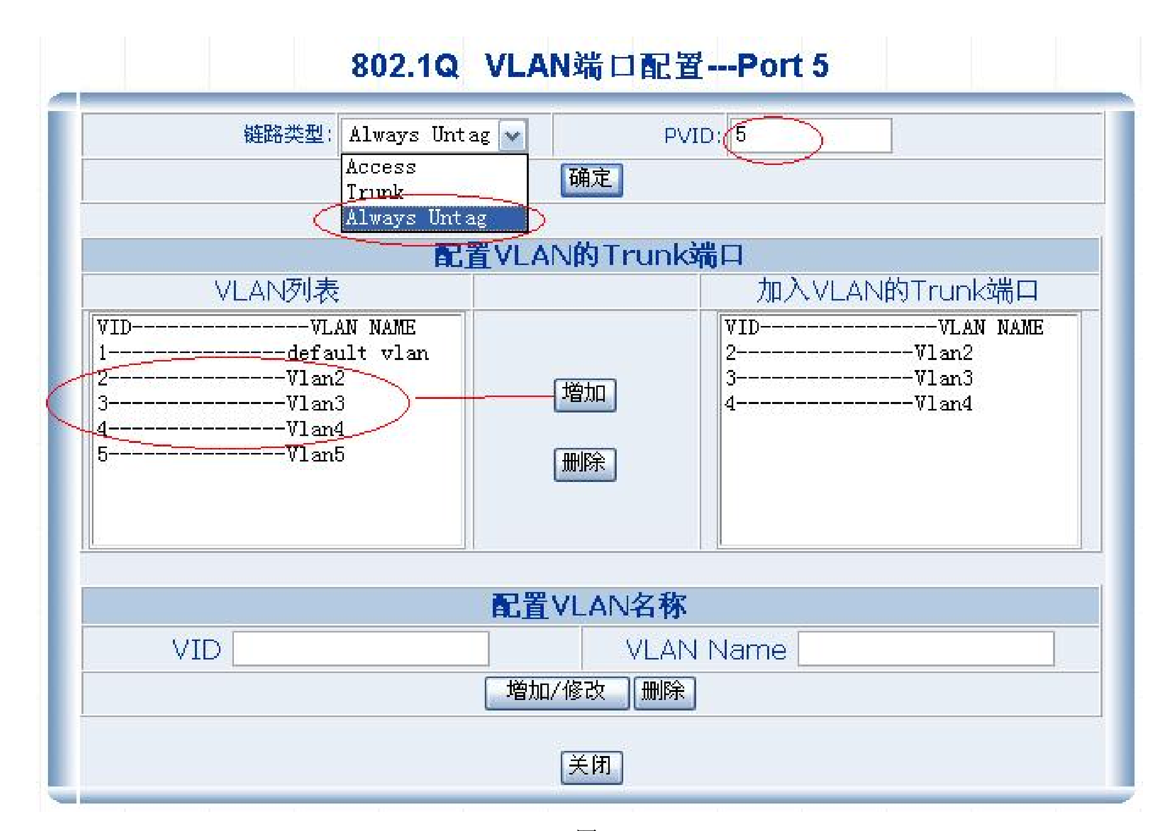


图 6.59

6.4.5 MAC 地址绑定

6.4.5.1 MAC 地址绑定原理

MAC地址绑定是Netcore 7324NSW二四层交换机支持的一项基于端口的安全技术。一般情况下，MAC地址表是交换机根据所连接的网络设备，通过源地址学习自动建立起来，但网络管理员也可以手动在表中加入特定网络设备的MAC地址,使之与交换机的相应的端口绑定，被绑定后的网络设备只能通过绑定了的交换机端口访问交换机，这样就大大提高端口安全性。增加了为每个VLAN记录一张单独的MAC地址表，将VLAN，端口，和MAC地址一对一,端口与MAC地址绑定后，只在对应的VLAN里有效。

6.4.5.2 Netcore 7324NSW 二四层交换机的 MAC 地址绑定配置

例如：将一台MAC地址为00-E0-4F-48-3A-7E的设备限制在7324NSW的1号端口上使用，具体操作如下：

在“MAC地址”框中输入00-E0-4F-48-3A-7E，然后在“端口号”框选中“PORT1”，点击“增加”。

MAC地址绑定

绑定新的MAC地址	
MAC地址	端口
00-E0-4F-48-3A-7E	port1

增加

查看绑定的MAC地址条目		
MAC地址	端口	删除

图 6.60

MAC地址绑定

绑定新的MAC地址	
MAC地址	端口
	port1

增加

查看绑定的MAC地址条目		
MAC地址	端口	删除
00-E0-4F-48-3A-7E	port1	删除

图 6.61

6.4.6 MAC 地址过滤

6.4.6.1 MAC 地址过滤原理

MAC地址过滤是交换机的另一项网络安全技术。用户可以自行把网络设备的属于该VLAN的MAC地址添加到MAC地址过滤表中，那过滤后的MAC地址，只在对应的VLAN中有效，被添加到MAC地址过滤表中的网络设备将无法访问交换机。

6.4.6.2 Netcore7324NSW 二四层交换机的 MAC 地址过滤配置

把连接在7324NSW二四层交换机的属于VLAN2的一台PC的MAC地址（PC网卡的MAC地址为00-E0-4F-48-3A-7E）进行过滤，具体操作如下：

在“MAC地址”框中输入00-E0-4F-48-3A-7E，点击“增加”，如下图所示：

MAC地址过滤

过滤新的MAC地址	
MAC地址	VID
00-E0-4F-48-3A-7E	2
增加	

当前过滤的M A C 地址		
MAC地址	VID	删除

图 6.62

MAC地址过滤

过滤新的MAC地址	
MAC地址	VID
增加	

当前过滤的M A C 地址		
MAC地址	VID	删除
00-E0-4F-48-3A-7E	2	删除

图 6.63

6.4.7 MAC 地址学习

6.4.7.1 MAC 地址学习原理

MAC地址学习是Netcore 7324NSW二四层交换机的另一项网络安全技术。用户可以自行选择针对每一个端口开启和关闭MAC地址学习。

6.4.7.2 Netcore 7324NSW 二四层交换机的 MAC 地址学习配置

在端口列表中输入需要进行管理的端口号，在“MAC地址学习”中选择该端口的学习状态Enable/Disable。

MAC地址学习

MAC地址学习	
端口列表	MAC地址学习
	Disable
增加	

察看端口MAC地址学习	
端口	MAC地址学习
Port1	Enable
Port2	Enable
Port3	Enable
Port4	Enable
Port5	Enable
Port6	Enable
Port7	Enable
Port8	Enable
Port9	Enable
Port10	Enable
Port11	Enable
Port12	Enable
Port13	Enable
Port14	Enable

图 6.64

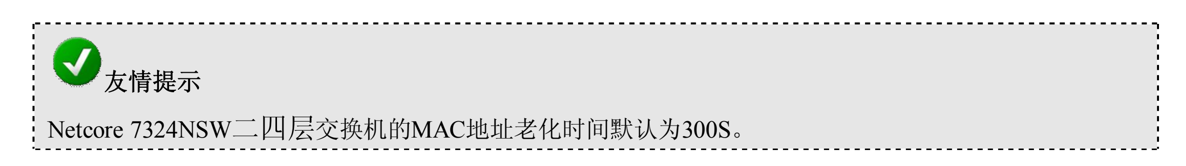
6.4.8 MAC 地址老化

MAC条目在交换机中如果一直未激活或未触发，在此可以设定MAC地址条目在交换机中的生存时间，单位“秒”。

MAC地址老化



图 6.65



6.5 QoS

6.5.1 QoS 简介

传统的分组网络对所有报文都无区别的等同对待。每个交换机/路由器对所有的报文采用先入先出的策略FIFO处理，尽最大的努力Best-Effort将报文送到目的地，但对报文传送的延时、延时抖动等传输性能不提供任何承诺和保证。

随着计算机网络的高速发展，对带宽、延迟、抖动敏感的语音、图像、重要数据越来越多地在网上传输。这样一方面使得网上的业务资源极大地丰富，另一方面则由于经常遭遇网络拥塞，人们对网络传输的服务质量QoS Quality of Service提出了更高的要求。

以太网技术是当今被广泛使用的网络技术。目前，以太网不仅成为各种独立的局域网中的主导技术，许多以太网形式的局域网也成为了Internet 的组成部分。而且随着以太网技术的不断发展，以太网接入方式也将成为广大普通Internet 用户的主要接入方式之一。因此要实现端到端的全网QoS解决方案，不可避免地要考虑以太网上的QoS业务保证的问题。这就需要以太网交换设备应用以太网QoS技术，对不同类型的业务流提供不同等级的QoS保证。尤其是能够支持那些对延时和抖动要求较高的业务流。

6.5.1.1 QoS 相关术语和概念

- **流：**流即业务流traffic 指所有通过交换机的报文。
- **流分类：**流分类traffic classification是指采用一定的规则识别出符合某类特征的报文。分类规则classification rule指配置管理员根据管理需求配置的规则。分类规则很简单，一般的分类依据都局限在封装报文的头部信息。
- **优先级标记：**以太网交换机可为特定报文提供优先级标记的服务，标记内容包括DSCP 802.1p等这些优先级标记分别适用于不同的QoS模型在不同的模型中被定义。
- **队列调度：**当网络拥塞时，必须解决多个报文同时竞争使用资源的问题。通常采用队列调度加以解决。这里介绍3种各具特色的队列调度算法：严格优先级SP（Strict-Priority）加权平均优先级（WRR：Weighted Round Robin）调度算法。

下面用简单的例子对比了在网络发生拥塞时，报文在无QoS保证和有QoS保证网络中的不同处理过程。

- 下图所示为发生拥塞时，网络设备的一个接口在不支持QoS的情况下，报文的发送情况：

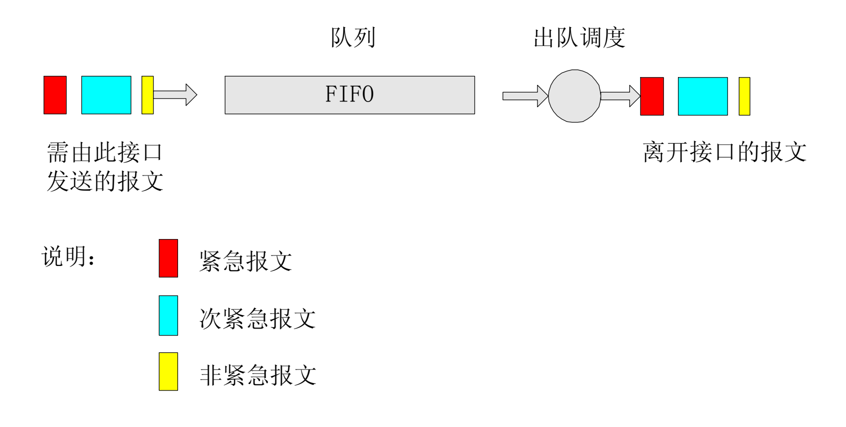


图 6.66

所有要从该接口输出的报文，按照到达的先后顺序进入接口的FIFO队列尾部，而接口在发送报文时，从FIFO（First in First out，先入先出）队列的头部开始，依次发送报文，所有的报文在发送过程中，没有任何区别，也不对报文传送的质量提供任何保证。

- 下图是一个用SQ（Strict Queuing）优先队列来支持QoS的报文发送情况：

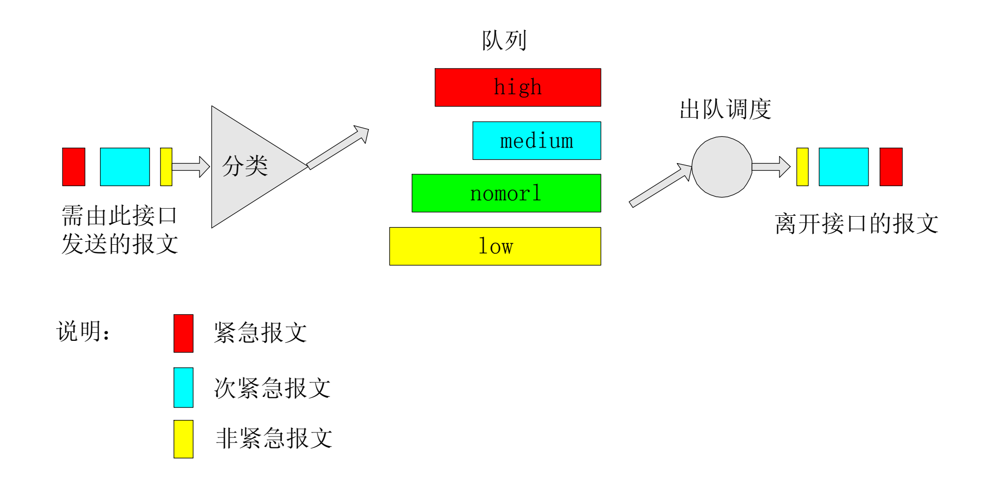


图 6.67

在报文到达接口后，首先对报文进行分类，然后按照报文所属的类别让报文进入所属队列的尾部，在报文发送时，按照优先级，总是在所有优先级高的队列发送完毕后，再发送低优先级队列中的报文。这样在每次发送报文时，总是将优先级高的报文先发出去，保证了属于较高优先级队列的报文有非常低的时延，其报文的丢失率和通过率这两个性能指标在网络拥塞时也可以有一定的保障。

- 下图是一个用WRR（Weighted Round Robin）加权平均优先级队列支持QoS的报文发送情况：

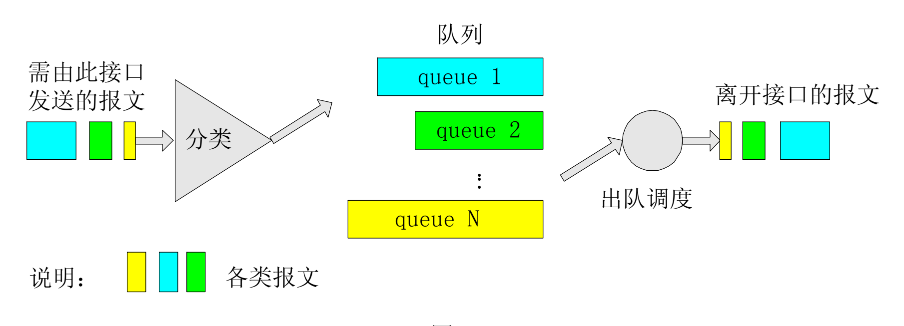


图 6.68

WRR是按照对列的权重进行对列调策略，对列对应的权重越大，该队列中的数据包越能优先转发，这在保证公平的基础上对不同优先级的业务体现优先转发的特性。

QoS旨在针对各种应用的不同需求，为其提供不同的服务质量，例如：提供专用带宽、减少报文丢失率、降低报文传送时延及时延抖动等。为实现上述目的，QoS提供了下述功能：

- 报文分类和着色
- 避免和管理网络拥塞
- 流量监管和流量整形
- QoS信令协议

6.5.1.2　QoS 的应用

QoS可以控制各种网络应用和满足各种网络应用要求，如：

- 控制资源：如可以限制骨干网上FTP使用的带宽，也可以给数据库访问以较高优先级。
- 可裁剪的服务：对于ISP（Inernet Service Provider，Internet服务提供商），其用户可能传送语音、视频或其他实时业务，QoS使ISP能区分这些不同的报文，并提供不同服务。
- 多种需求并存：可以为时间敏感的多媒体业务提供带宽和低时延保证，而其他业务在使用网络时，也不会影响这些时间敏感的业务。

在一个网络中，需要以下的三个部分来完成端到端的QoS：

- 各网络元件（路由器、以太网交换机等）支持QoS，提供队列调度、流量整形等功能。
- 信令技术来协调端到端之间的网络元件为报文提供QoS。
- QoS控制和管理端到端之间的报文在一个网络上的发送。而每个网络元件提供如下功能：
- 报文分类，对不同类别的报文提供不同的处理。
- 队列管理和调度来满足不同应用要求的不同服务质量。
- 流量监管和流量整形限制和调整报文输出的速度。
- 接入控制来确定是否允许用户信息流使用网络资源。

6.5.2　QoS 配置

Netcore 7324NSW二四层网管交换机支持802.1P、端口优先级；支持八个优先级队列；支持严格优先级队列与加权循环队列两种对列调度方式。


友情提示

流分类技术优先级：支持DSCP、802.1P、端口优先级

6.5.2.1　802.1p-队列映射

交换机对802.1P数据帧中携带的优先级字段映射成所对应的队列作为流分类的条件

具体操作：在“802.1p Priority (0-7)”输入框中输入优先级分类，选择映射的队列优先级，点击确定完成配置。

1p-队列映射

设置1p-队列映射	
802.1p Priority (0-7)	队列 (0-7)
2	3

确定

查看1p-队列映射	
802.1p Priority	队列
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

图 6.69

1p-队列映射

设置1p-队列映射	
802.1p Priority (0-7)	队列 (0-7)

确定

查看1p-队列映射	
802.1p Priority	队列
0	0
1	1
2	3
3	3
4	4
5	5
6	6
7	7

图 6.70

6.5.2.2 端口默认优先级

交换机对于所有在这个端口接收的报文将以端口设置的优先级作为流分类的条件。

具体操作：输入进行优先级设置的端口号，输入优先级。

端口默认优先级

设置端口默认优先级

端口列表	优先级（0-7）
4	5

确定

查看端口默认优先级

端口	优先级
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0

图 6.71

端口默认优先级

设置端口默认优先级	
端口列表	优先级（0-7）
确定	

查看端口默认优先级	
端口	优先级
1	0
2	0
3	0
4	5
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0

图 6.72

6.5.2.3　队列调度

1：队列调度的概念

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题。通常采用队列调度加以解决。这里介绍2种各具特色的队列调度算法：严格优先级SP（Strict-Priority） 队列调度算法加权轮循WRR Weighted Round Robin调度算法和带最大时延的WRR 调度算法。

- SP 调度算法（Always High）

SP 队列调度算法是针对关键业务型应用设计的关键业务有一重要的特点，即在拥塞发生时要求优先获得服务以减小响应的延迟。以端口有8个输出队列为例优先队列将端口的8个输出队列分成8 类分别为高优先队列中优先队列正常优先队列和低优先队列（依次为8~0队列），它们的优先级依次降低。在队列调度时，SP严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。这样，将关键业务的分组放入较高优先级的队列，将非关键业务如E-Mail的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。

SP 的缺点是拥塞发生时如果较高优先级队列中长时间有分组存在那么低优先级队列中的报文就会由于得不到服务而“饿死”。

- WRR 调度算法

交换机的端口支持8个输出队列，WRR队列调度算法在队列之间进行轮流调度保证每个队列

都得到一定的服务时间。WRR 队列还有一个优点是，虽然多个队列的调度是轮循进行的，但对每个队列不是固定地分配服务时间片——如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

2：Netcore 7324NSW 二四层交换机队列调度的设置

当网络拥塞时，必须解决多个报文同时竞争使用资源的问题，通常采用队列调度加以解决。交换机依据报文的COS优先级进行入队列操作。

严格优先级队列SQ保证高优先级业务总是在低优先级业务之前处理；WRR是一种加权循环队列调度

机制，首先处理高优先级，但在处理高优先级业务时，较低优先级的业务并没有被完全阻塞，而是按一定的比例同时进行。Netcore 7324NSW二四层交换机允许严格优先级队列与加权循环队列同时存在。

1）根据权重的高低，来排列转发数据的先后



队列	权重
Queue 7	8
Queue 6	7
Queue 5	6
Queue 4	5
Queue 3	4
Queue 2	3
Queue 1	2
Queue 0	1

图 6.73

2）永远执行最高优先级的，除非最高优先级没有数据了，才会往下面依次转发。在低优先级转发数据的时候，只要发现最高优先级又有数据了，那马上就又转发最高优先级的。

队列调度

设置队列调度策略

队列调度策略 Always High

确定

查看队列权重

队列	权重
Queue 7	8
Queue 6	7
Queue 5	6
Queue 4	5
Queue 3	4
Queue 2	3
Queue 1	2
Queue 0	1

图 6.74

6.5.2.4 信任模式

选择任一一种模式，做为QOS的使用的依据



图 6.75

6.6 网络分析

6.6.1 端口镜像

端口镜像提供端口监视功能，它把指定端口的数据包复制到监控端口。允许用户自行设置一个监视管理端口来监视被监视端口的数据。监视到的数据可以通过 PC 上安装的端口监视软件反映，如 EtherPeek NX、SpyNet 等，用户把监视到的数据进行分析就可以知道被监视端口情况，从而进行网络检测、监控和故障排除。

设置端口 1 去监视从端口 5 出去数据到端口 6 进来的数据：

具体操作：在流量捕获配置下，“捕获状态”设置为“Enable”，“捕获端口”框选中“Port1”，点击“确定”。然后在“被监视源端口列表”输入“5”，在“被监视目的端口列表”输入“6”，点击“增加”，查看捕获器中会显示配置的条件。如图所示：

端口镜像

流量捕获配置	
捕获端口：	Port1
捕获状态：	Enable
确定	

镜像端口配置	
被捕获源端口列表	被捕获目的端口列表
5	6
确定	

图 6.76

6.6.2 QOS 统计器

根据配置的 ACL 条件，把符合此条件的数据包的数量统计下来。它是针对用户感兴趣的报文作统计分析。

具体操作：先在“ACL”中配置，其中“允许/禁止：”设置为“PERMIT”，然后设置“统计器的名称” 后，就能在 QOS 统计器中查看到这个设定好的统计器。 查看此统计器来对感兴趣的数据包进行统计分析。

QoS统计器

统计器名称	包个数
1	405
2	442
3	400

刷新

图 6.77

6.6.3 ARP 攻击日志

直观的显示出网络中 ARP 攻击的信息，方便迅速的找到 ARP 攻击源

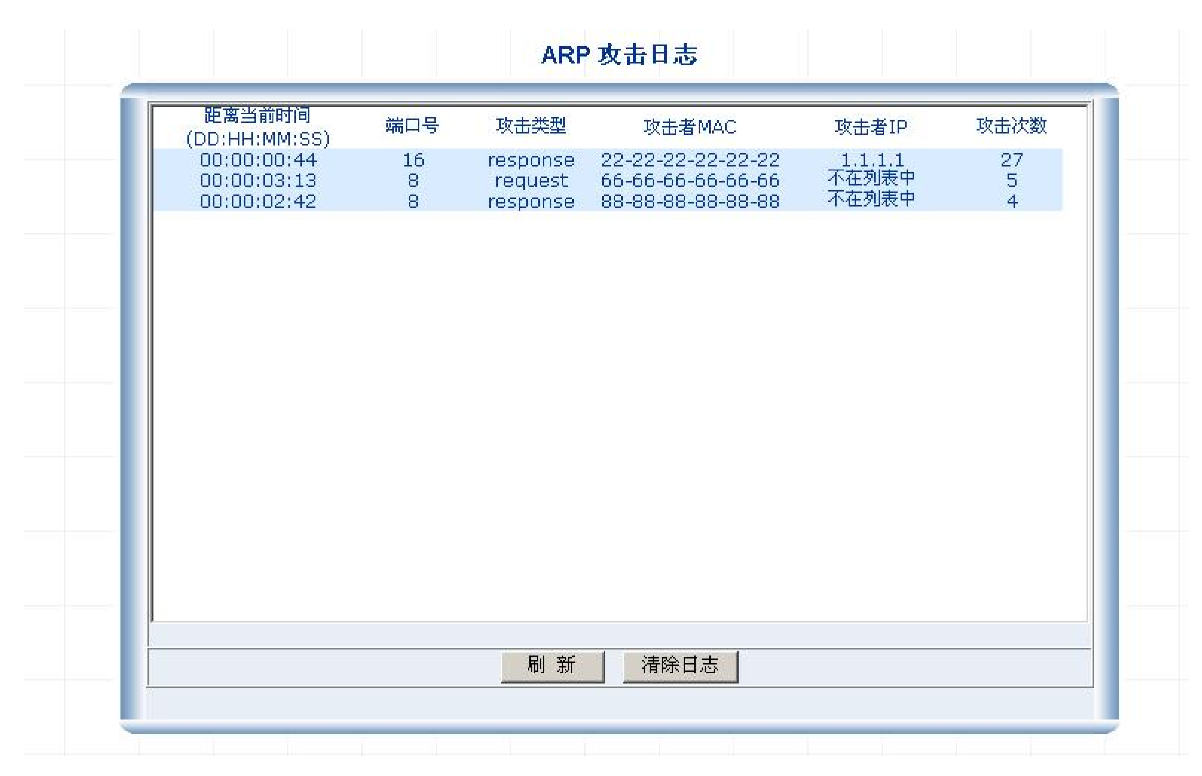


图 6.78

6.7 网络设备保护

6.7.1 主机安全保护

在所选择的安全策略下，设置主机的权限。

6.7.1.1 自动搜索网络设备

在添加网络设备选项中，选择自动搜索网络设备，可以添加一个或者一段IP地址，自动搜索出MAC地址，缺省状态为主机，未绑定。

主机安全保护

主机安全保护

安全策略：所有主机能访问网络

确定

添加网络设备

自动搜索网络设备

起始IP地址	结束IP地址	VLAN
192.168.2.8	192.168.2.8	1

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定0条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.79

设置成功后，您可以根据您的实际情况设置各个属性。

主机安全保护

主机安全保护

安全策略：所有主机能访问网络

确定

添加网络设备

自动搜索网络设备

起始IP地址	结束IP地址	VLAN

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定0条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
192.168.2.8	00-E0-4C-82-66-79		1	21	主机	未绑定	0	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.80

设备属性配置

设备属性	
IP地址：	192.168.2.8
MAC地址：	00-E0-4C-82-66-79
VLAN：	1
端口：	23
设备名称：	
设备类型：	主机 路由器 DHCP Server
路由器IP：	
带宽限制：	0 kbps/s
重新学习	确定

图 6.81

注：如您配置成功后出现以下情况（有红色条目），即表示有多个相同的 IP 地址回应了交换机发出的 ARP 报文，那有可能此 IP 对应的主机受到 ARP 攻击。如下：多个 1.1.1.5 的 IP 地址为回应了此交换机发出的报文。

主机安全保护

主机安全保护

安全策略：所有主机能访问网络

确定

添加网络设备

自动搜索网络设备

起始IP地址	结束IP地址	VLAN

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流　已绑定0条　一键绑定　一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
1.1.1.1	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.2	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.3	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.4	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.5	CC-CC-CC-CC-CC-CC		1	18	主机	未绑定	0	删除
1.1.1.6	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.7	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.8	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.9	22-22-22-22-22-22		1	2	主机	未绑定	0	删除
1.1.1.10	22-22-22-22-22-22		1	2	主机	未绑定	0	删除

第1页 共60页 跳转到第 页 确定　上页　下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.82

红色条目与“一键绑定”间的关系：

- 如在搜索后有红色的条目,再绑定这个红色条目的话,就没有红色条目了

主机安全保护

主机安全保护

安全策略：所有主机能访问网络

确定

添加网络设备

自动搜索网络设备

起始IP地址	结束IP地址	VLAN

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定600条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽 (kbps/s)	删除
1.1.1.1	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.2	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.3	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.4	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.5	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.6	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.7	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.8	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.9	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.10	22-22-22-22-22-22		1	2	主机	已绑定	0	删除

第1页 共60页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.83

- 如果一个条目已经绑定了,再搜索有冲突的话,就会在绑定的情况下是红色.

主机安全保护

主机安全保护

安全策略：所有主机能访问网络

确定

添加网络设备

自动搜索网络设备

起始IP地址	结束IP地址	VLAN

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流　已绑定600条　一键绑定　一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
1.1.1.1	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.2	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.3	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.4	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.5	CC-CC-CC-CC-CC-CC		1	18	主机	已绑定	0	删除
1.1.1.6	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.7	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.8	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.9	22-22-22-22-22-22		1	2	主机	已绑定	0	删除
1.1.1.10	22-22-22-22-22-22		1	2	主机	已绑定	0	删除

第1页 共60页 跳转到第 页 确定　上页　下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.84

6.7.1.2 手动添加网络设备

手动设置您所需要的配置，注意其中的带宽限制是指主机带宽限制，是主机到路由器入口的速度。

主机安全保护

主机安全保护			
安全策略： 所有主机能访问网络			
确定			

添加网络设备			
手动添加网络设备			
IP地址：	192.168.2.8	MAC地址：	00-11-22-33-44-55
VLAN：	1	端口：	23
设备类型：	主机 路由器 DHCP Server	设备名：	
		带宽限制(kbyte/s)：	
		路由器IP：	
确定			

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定0条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.85

主机安全保护

主机安全保护

安全策略： 所有主机能访问网络

确定

添加网络设备

手动添加网络设备

IP地址：		MAC地址：	
VLAN：		端口：	
设备类型：	主机 路由器 DHCP Server	设备名：	
		带宽限制(kbyte/s)：	
		路由器IP：	

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定1条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
192.168.2.8	00-11-22-33-44-55		1	23	主机	已绑定	0	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合組端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.86

6.7.1.3 批量限流

设置一段 IP 的速度，减少重复设置的烦琐

- 设置 IP 为 192.168.2.8 的类型为主机属性；IP 为 192.168.2.16 的类型为路由器属性

主机安全保护

主机安全保护
安全策略：所有主机能访问网络
确定

添加网络设备		
自动搜索网络设备		
起始IP地址	结束IP地址	VLAN
确定		

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流　已绑定2条　一键绑定　一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
192.168.2.8	00-11-22-33-44-55		1	23	主机	已绑定	0	删除
192.168.2.16	00-22-33-44-55-66		1	11	路由器	已绑定	0	删除

第1页 共1页 跳转到第 页 确定　上页　下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.87

- 设置一段 IP 从 192.168.2.5 到 192.168.2.10 的带宽限制为 50Kbyte/s。



图 6.88

- 192.168.2.8 在此设置的 IP 段范围内，设置成功后，其速度为 50Kbyte/s

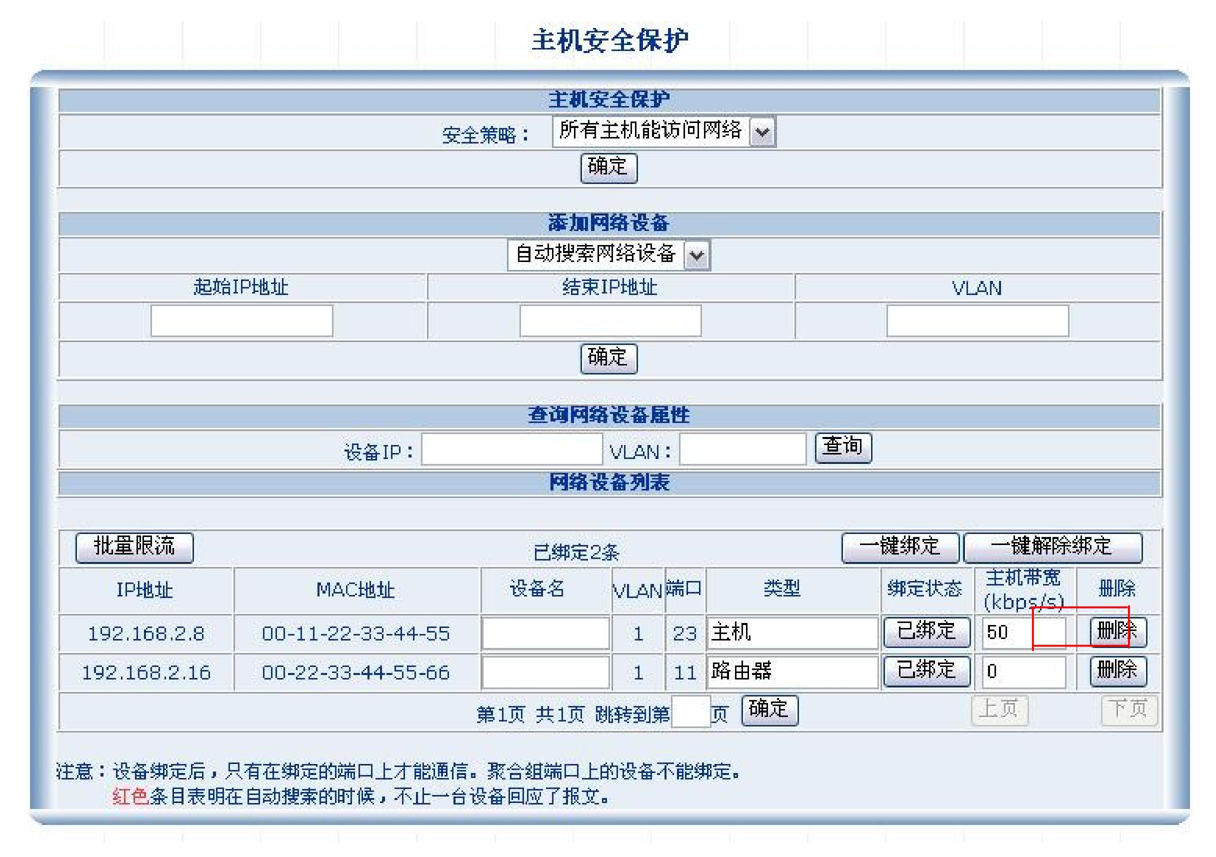


图 6.89

6.7.2 网络设备保护

通过此保护程序，确保您网络中的使用的每个设备安全，更好的保护您的系统。

网络设备保护

主机带宽限制

说明：启用本功能将会对主机到路由器之间的速度进行限制，请首先配置主机带宽限制。

☑ 启用主机←→路由器带宽限制

确定

DHCP Server保护

说明：本功能对合法DHCP Server进行保护，防止非法DHCP Server的干扰。请首先配置合法DHCP Server（网络设备属性为DHCP Server）。

☐ 启用DHCP Server保护功能

确定

路由器端口速度限制

IP地址	速度限制（100－1000000）
	（kbps/s）

确定

查看路由器端口速度限制

IP地址	设备名	端口	速度限制（kbps/s）	删除

图 6.90

- 在主机安全保护里，如果您设置主机的带宽限制，请到此处开启总开关。主机带宽限制，是指从主机出口出去，经过交换机到路由器的入口的速度。

例；设置主机 192.168.2.8 出口到路由器 192.168.2.16 入口处的带宽。

1. 添加 IP 为 192.168.2.16 的网络设备。设备类型为路由器。

主机安全保护

主机安全保护

安全策略：所有主机能访问网络 确定

添加网络设备

手动添加网络设备

IP地址：	192.168.2.16	MAC地址：	00-22-33-44-55-66
VLAN：	1	端口：	11
设备类型：	主机 路由器 DHCP Server	设备名：	
		带宽限制(kbyte/s)：	
		路由器IP：	

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定0条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.91

主机安全保护

主机安全保护

安全策略：所有主机能访问网络 确定

添加网络设备

自动搜索网络设备

起始IP地址	结束IP地址	VLAN

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定1条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
192.168.2.16	00-22-33-44-55-66		1	11	路由器	已绑定	0	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.92

2. 添加IP为192.168.2.8的网络设备。设备类型为主机，带宽速度为20K。

主机安全保护

主机安全保护

安全策略： 所有主机能访问网络

确定

添加网络设备

手动添加网络设备

IP地址：	192.168.2.8	MAC地址：	00-11-22-33-44-55
VLAN：	1	端口：	5
设备类型：	主机 路由器 DHCP Server	设备名：	
		带宽限制(kbyte/s)：	20
		路由器IP：	192.168.2.16

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定1条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
192.168.2.16	00-22-33-44-55-66		1	11	路由器	已绑定	0	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.93

主机安全保护

主机安全保护

安全策略： 所有主机能访问网络

确定

添加网络设备

自动搜索网络设备

起始IP地址	结束IP地址	VLAN

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定2条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
192.168.2.8	00-11-22-33-44-55		1	5	主机	已绑定	20	删除
192.168.2.16	00-22-33-44-55-66		1	11	路由器	已绑定	0	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.94

这样，您就可以设置好，从主机 192.168.2..8 到路由器 192.168.2.16 的端口带宽速度为 20K。

- 在网络设备属性中，如果您选择了 DHCP Server，请到此处开启总开关，这样，您设置的才会其效，才能对网络设备中的 DHCP Server 进行保护。

网络设备保护

主机带宽限制

说明：启用本功能将会对主机到路由器之间的速度进行限制，请首先配置主机带宽限制。

☐ 启用主机←→路由器带宽限制

确定

DHCP Server保护

说明：本功能对合法DHCP Server进行保护，防止非法DHCP Server的干扰。请首先配置合法DHCP Server（网络设备属性为DHCP Server）。

☑ 启用DHCP Server保护功能

确定

路由器端口速度限制

IP地址	速度限制（100-1000000）
	（kbps/s）

确定

查看路由器端口速度限制

IP地址	设备名	端口	速度限制（kbps/s）	删除

图 6.95

- 路由器端口速度限制：交换机特定端口到路由器出口的速度。

主机安全保护

主机安全保护

安全策略： 所有主机能访问网络

确定

添加网络设备

手动添加网络设备

IP地址：		MAC地址：	
VLAN：		端口：	
设备类型：	主机 路由器 DHCP Server	设备名：	
		带宽限制(kbyte/s)：	
		路由器IP：	192.168.2.16

确定

查询网络设备属性

设备IP： VLAN： 查询

网络设备列表

批量限流 已绑定1条 一键绑定 一键解除绑定

IP地址	MAC地址	设备名	VLAN	端口	类型	绑定状态	主机带宽(kbps/s)	删除
192.168.2.16	00-22-33-44-55-66		1	11	路由器	已绑定	0	删除

第1页 共1页 跳转到第 页 确定 上页 下页

注意：设备绑定后，只有在绑定的端口上才能通信。聚合组端口上的设备不能绑定。
红色条目表明在自动搜索的时候，不止一台设备回应了报文。

图 6.96

网络设备保护

主机带宽限制
说明：启用本功能将会对主机到路由器之间的速度进行限制，请首先配置主机带宽限制。
☑ 启用主机←→路由器带宽限制
确定

DHCP Server保护
说明：本功能对合法DHCP Server进行保护，防止非法DHCP Server的干扰。请首先配置合法DHCP Server（网络设备属性为DHCP Server）。
☐ 启用DHCP Server保护功能
确定

路由器端口速度限制	
IP地址	速度限制（100－1000000）
192.168.2.16	200 （kbps/s）
确定	

查看路由器端口速度限制				
IP地址	设备名	端口	速度限制（kbps/s）	删除

图 6.97

网络设备保护

主机带宽限制
说明：启用本功能将会对主机到路由器之间的速度进行限制，请首先配置主机带宽限制。
☑ 启用主机←→路由器带宽限制
确定

DHCP Server保护
说明：本功能对合法DHCP Server进行保护，防止非法DHCP Server的干扰。请首先配置合法DHCP Server（网络设备属性为DHCP Server）。
☐ 启用DHCP Server保护功能
确定

路由器端口速度限制	
IP地址	速度限制（100－1000000）
192.168.2.16	（kbps/s）
确定	

查看路由器端口速度限制				
IP地址	设备名	端口	速度限制（kbps/s）	删除
192.168.2.16		2	200	删除

图 6.98

6.7.3 应用程序优先级

根据设置的所需应用，来决定其处理级别的高低。

例：一般来说，如果遇到内网有人下载 BT，那是肯定会很快的把带宽给占满的，这样，就有可能影响内网的其他用户上网。甚至连 QQ 发送消息或者 QQ 语音都无法正常使用。那为了满足大部分用户的 QQ 使用，您就可以把它的优先级设置为高优先级，既转发数据的时候，优先转发关于 QQ 的。做到了就算有人使用 BT，对 QQ 一些简单的操作也不会受影响。

应用程序优先级

程序优先级模板应用

应用程序模板： QQ语音 高优先级

确定

用户定义应用程序优先级

名称:

协议: TCP UDP

优先级: 高优先级

确定

查看程序优先级应用

名称	端口列表	优先级	删除

图 6.99

当然，您也可以根据您的需要，在用户定义应用程序优先级里做设置，我们提供了针对端口限制的优先级配置。

应用程序优先级

程序优先级模板应用

应用程序模板： QQ语音 高优先级

确定

用户定义应用程序优先级

名称:

协议: TCP UDP

TCP端口:

UDP端口:

优先级: 高优先级

高优先级
中优先级
普通优先级
低优先级

查看程序优先级应用

名称	端口列表	优先级	删除

图 6.100

第七章 常见问题和处理方法

7.1 开机故障

7.1.1 电源故障

首先查看交换机的电源指示灯，如果指示灯熄灭，可能是外电源连接不良，请确定电源接线板供电是否正常，并检查电源线与电源接线板、以及与 Netcore 7324NSW 交换机的连接是否稳定可靠。

7.1.2 交换机启动故障

如果不能从 CONSOLE 端口连接的终端屏幕上观察到交换机成功启动，请按下列步骤检查：

- 检查所使用的终端软件设定的串口号是否正确：通常PC上带有2个串口，分别是COM1和COM2；
- 检查所使用的终端软件的通讯配置是否是：38400bps、8数据位、1停止位、无奇偶校验、无流控；
- 检查PC上的串行口工作是否正常：可以使用串口鼠标来检测串口硬件有没有故障；
- 确认用户的Windows操作系统中有没有其他程序在使用该串口；Windows操作系统不允许多个程序同时使用一个串口；

7.2 以太链路故障

7.2.1 概述

以太链路故障可能体现出多种现象：

- 无法和PC网卡连接，链路状态指示灯显示不能正常连接；
- 端口可以与PC网卡连接（链路状态指示灯正常），但无法和其他某些端口通讯；
- 端口可以与PC网卡连接（链路状态指示灯正常），但通过该端口无法对Netcore 7324NSW交换机进行管理。
- 可以把这类故障大致分为两大类型：
  1：Link-Error，链路两端无法建立物理连接，表现出的现象是链路状态指示灯不正常。
  2：配置冲突，表现出的现象是链路状态指示灯正常，但无法和其他端口进行通讯。

7.2.2 链路状态指示灯显示不正常(Link-Error)

出现这种情况时，请按照下列步骤进行检查：

- 查看链路另一端是否良好地连接到PC网卡或其他以太接口上；
- 检查连接电缆及两端的RJ45接头是否有锈蚀或损坏；
- 使用WEB方式(检查该端口的通讯配置（双工、速度），确定其配置是否与链路另一端相匹配。


重要提示

当链路两端均强制设置双工和速度时，如果设置不匹配，是无法建立连接的。

7.2.3 链路状态指示灯显示正常但无法通讯

出现这种情况时，请按照下列步骤进行检查：

- 使用WEB方式（见端口状态查询）检查该端口是否被停止，如果显示该端口被停用，则使用WEB方式（见端口配置中的关闭/打开）打开该端口；
- 使用WEB方式检查该端口是否在VLAN设置中与其他端口隔离；端口只能和同一个VLAN内的成员端口进行通讯。

7.3 无法远程登陆管理交换机

7.3.1 概述

请按照下面的步骤对 Netcore 7324NSW 交换机进行检查：

- 按照7.1.2 交换机启动故障介绍的方法检查Netcore 7324NSW交换机是否成功启动；
- 按照7.2 以太链路故障介绍的方法检查有无链路故障；
- 使用PING程序检测Netcore 7324NSW交换机有无回应：如果没有回应，则检查Netcore 7324NSW交换机和PC的IP地址配置是否正确；如果有回应，则可根据HTTP连接反馈信息来判断故障原因。

7.3.2 检查 IP 地址设置

请按照下面的步骤对 Netcore 7324NSW 交换机进行检查：

- 检查PC的IP地址、子网掩码以及默认网关设置是否是你期望的设置：在Windows命令行方式下输入ipconfig查看PC的IP地址配置；
- 检查Netcore 7324NSW交换机的IP地址、子网掩码以及默认网关设置是否是你期望的设置：在CONSOLE方式下使用检查Netcore 7324NSW交换机的IP地址设置；
- 检查PC和Netcore 7324NSW交换机的IP地址是否被其它设备占用；

7.3.3 检查远程登录帐号

用户使用 WEB 方式远程登录时，如果 Netcore 7324NSW 交换机连续要求输入帐号和密码，这可能是输入的帐号不存在或输入的密码错误。


温馨提示

控制台（CONSOLE）模式的配置方法的配置方法，请查阅7324NSW用户手册。

附 录

附录 A 配件清单

检查包装盒里应有以下配件：

- 一台Netcore 7224NSW
- 一根串口线
- 一个电源线
- 一本用户手册
- 一张Netcore保修卡



温馨提示

如果发现物品有损坏或者遗漏，请及时与当地Netcore经销商联系。

附录 B FCC 认证

本设备已经进行过检测，符合 FCC 第 15 部分中的 B 级数字设备标准。该标准详细规定了安装于居住环境的无线设备可能产生的有害干扰的各项安全参数。

本设备产生、使用，并发射一定频率的无线电波。如果违反说明书中的要求进行安装，可能会造成有害的无线电干扰。但是，也不保证某种安装状态一定不产生干扰。如果本设备确实对收音或电视产生了干扰，并且通过关闭或打开本设备确认了此干扰的存在，用户可以尝试通过以下方式来减小干扰：

- 调整接收天线的位置和方向；
- 加大接收天线与本设备之间的距离；
- 将本设备接入与被干扰设备不同的电源插座；
- 咨询经销商或者有经验的收音/电视技术人员，以获取帮助。

为确保符合 FCC 对辐射的规定，应使用干扰屏蔽连接线进行连接。

在未经相关权威机构明确认可的情况下，应避免任何对本产品的改动或调整。

本设备符合 FCC 第 15 部分的规定。其操作符合以下两种情况：

- 此设备不会造成有害干扰；
- 此设备可以抵抗自身受.到的干扰，包括可能引起操作错误的干扰。

附录 C　技术支持

技术支持

支持中心电话：400-8101616
网地：http://www.netcoretec.com
E-mail： support@netcoretec.com
周一到周五，早09：00---晚19：00
周六，早10：00---晚17：00